



WiNG 5.9.2 Wireless Controller, Service Platform, and Access Point

CLI Reference Guide

Copyright © 2018 Extreme Networks, Inc. All rights reserved.

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see:

www.extremenetworks.com/company/legal/trademarks

Software Licensing

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at:

www.extremenetworks.com/support/policies/software-licensing

Support

For product support, phone the Global Technical Assistance Center (GTAC) at 1-800-998-2408 (toll-free in U.S. and Canada) or +1-408-579-2826. For the support phone number in other countries, visit: <http://www.extremenetworks.com/support/contact/>

For product documentation online, visit: <https://www.extremenetworks.com/documentation/>

Table of Contents

Preface	5
Text Conventions.....	5
Platform-Dependent Conventions.....	5
Providing Feedback to Us.....	6
Getting Help.....	6
Preface.....	7
ABOUT THIS GUIDE	8
ABOUT THIS GUIDE.....	8
INTRODUCTION	11
INTRODUCTION.....	11
USER EXEC MODE COMMANDS	25
USER EXEC MODE COMMANDS.....	25
PRIVILEGED EXEC MODE COMMANDS	105
PRIVILEGED EXEC MODE COMMANDS.....	105
GLOBAL CONFIG MODE COMMANDS	228
GLOBAL CONFIGURATION COMMANDS.....	228
COMMON COMMANDS	640
COMMON COMMANDS.....	640
SHOW COMMANDS	698
SHOW COMMANDS.....	698
PROFILE COMMANDS	857
PROFILES.....	857
AAA POLICY COMMANDS	1316
AAA-POLICY.....	1316
AUTO PROVISIONING POLICY	1336
AUTO-PROVISIONING-POLICY.....	1336
ASSOCIATION ACL POLICY	1355
ASSOCIATION-ACL-POLICY.....	1355
ACCESS LIST	1360
ACCESS-LIST.....	1360
DHCP POLICY	1428
DHCP-SERVER-POLICY.....	1428
FIREWALL POLICY	1483
FIREWALL-POLICY.....	1483
MiNT Security Policy	1513
MINT-POLICY.....	1513
MANAGEMENT POLICY	1519
MANAGEMENT-POLICY.....	1519
RADIUS POLICY	1551
RADIUS-POLICY.....	1551
RADIO QoS POLICY	1581
RADIO-QOS-POLICY.....	1581
ROLE POLICY	1594
ROLE-POLICY.....	1594
SMART RF POLICY	1629
SMART-RF-POLICY.....	1629
WIPS POLICY	1653

WIPS-POLICY.....	1653
WLAN QoS Policy.....	1675
WLAN-QOS-POLICY.....	1675
L2TPV3 Policy.....	1690
L2TPV3-POLICY.....	1690
Router Mode.....	1722
ROUTER-MODE.....	1722
Routing Policy.....	1738
ROUTING-POLICY.....	1738
AAA TACACS POLICY COMMANDS.....	1751
AAA-TACACS-POLICY.....	1751
MESHPOINT.....	1760
MESHPOINT.....	1760
PASSPOINT POLICY.....	1802
PASSPOINT POLICY.....	1802
CRYPTO CMP POLICY.....	1831
CRYPTO-CMP-POLICY.....	1831
other-cmp-related-commands.....	1840
ROAMING ASSIST POLICY.....	1843
ROAMING ASSIST POLICY.....	1843
BORDER GATEWAY PROTOCOL.....	1852
BORDER GATEWAY PROTOCOL.....	1852
CONTROLLER MANAGED WLAN USE CASE.....	1923
CREATING A FIRST CONTROLLER MANAGED WLAN.....	1923

Preface

This section discusses the conventions used in this guide, ways to provide feedback, additional help, and other Extreme Networks publications.

Text Conventions

The following tables list text conventions that are used throughout this guide.

Table 1: Notice Icons





Icon	Notice Type	Alerts you to...
	General Notice	Helpful tips and notices for using the product.
	Note	Important features or instructions.
	Caution	Risk of personal injury, system damage, or loss of data.
	Warning	Risk of severe personal injury.
<i>New!</i>	New Content	Displayed next to new content. This is searchable text within the PDF.

Table 2: Text Conventions

Convention	Description
Screen displays	This typeface indicates command syntax, or represents information as it appears on the screen.
The words enter and type	When you see the word “enter” in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says “type.”
[Key] names	Key names are written with brackets, such as [Return] or [Esc] . If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press [Ctrl]+[Alt]+[Del]
<i>Words in italicized type</i>	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.

Platform-Dependent Conventions

Unless otherwise noted, all information applies to all platforms supported by ExtremeXOS® software, which are the following:

- ExtremeSwitching® switches
- Summit® switches
- SummitStack™

When a feature or feature implementation applies to specific platforms, the specific platform is noted in the heading for the section describing that implementation in the ExtremeXOS command documentation (see the Extreme Documentation page at <http://documentation.extremenetworks.com>). In many cases, although the command is available on all platforms, each platform uses specific keywords. These keywords specific to each platform are shown in the Syntax Description and discussed in the Usage Guidelines sections.

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short [online feedback form](#). You can also email us directly at internalinfodev@extremenetworks.com.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

- **GTAC (Global Technical Assistance Center) for Immediate Support**
 - **Phone:** 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact
 - **Email:** support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- **Extreme Portal** — Search the GTAC knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.
- **The Hub** — A forum for Extreme customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Preface

This section discusses the conventions used in this guide, ways to provide feedback, additional help, and other Extreme Networks publications.



ABOUT THIS GUIDE

ABOUT THIS GUIDE

This manual supports the following access points, wireless controllers and service platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000



Note

In this document NX 9500 and NX 9510 are collectively referred to as NX 95XX.



Note

In this document NX 9600 and NX 9610 are collectively referred to as NX 96XX.

Notational Conventions

The following notational conventions are used in this document:

- Italics are used to highlight specific items in the general text, and to identify chapters and sections in this and related documents.
- Bullets (•) indicate:
 - lists of alternatives
 - lists of required steps that are not necessarily sequential
 - action items
- Sequential lists (those describing step-by-step procedures) appear as numbered lists

Understanding Command Syntax

<p><variable></p>	<p>Variables are described with a short description enclosed within a '<' and a '>' pair. For example, the command, <code>nx9500-6C8809>show interface ge 1</code> is documented as: <code>show interface ge <1-2></code> where:</p> <ul style="list-style-type: none"> • show - is the command - displays information • interface - is the keyword - represents the interface type • <1-2> - is the variable - represents the ge interface index value <p>Note: Since this output is from an NX 95XX service platform, which supports only two (2) GE interfaces, the index value is shown as <1-2>. This value will vary depending on the platform type.</p>
<p> </p>	<p>The pipe symbol. This is used to separate the variables/keywords in a list. For example, the command, <code>nx9500-6C8809> show</code> is documented as: <code>show [adoption bluetooth bonjour boot]</code> where:</p> <ul style="list-style-type: none"> • show - is the command - displays information • [adoption bluetooth bonjour boot] - indicates the different keywords that can be combined with the <i>show</i> command. However, only one of the above option can be used at a time. <pre>show adoption ... show bluetooth ... show bonjour ...</pre>
<p>[]</p>	<p>Of the different keywords and variables listed inside a '[' & ']' pair, only one can be used. Each choice in the list is separated with a ' ' (pipe) symbol. For example, the command, <code>nx9500-6C8809# clear ...</code> is documented as: <code>[clear [arp-cache bonjour cdp counters crypto event-history firewall gre ip ipv6 l2tpv3-stats lcp license lldp logging mac-address-table mint role rtls spanning-tree traffic-shape vrrp]</code> where:</p> <ul style="list-style-type: none"> • clear - is the command • [arp-cache cdp bonjour counters crypto event-history firewall gre ip ipv6 l2tpv3-stats lcp license lldp logging mac-address-table mint role rtls spanning-tree traffic-shape vrrp] - indicates that these keywords are available for this command. However, only one can be used at a time.

<p>{ }</p>	<p>Any command/keyword/variable or a combination of them inside a '{ & }' pair is optional. All optional commands follow the same conventions as listed above. However, they are displayed italicized.</p> <p>For example, the command, <code>nx9500-6C8809> show adoption ...</code> is documented as: <code>show adoption info {on <DEVICE-NAME>}</code> here:</p> <ul style="list-style-type: none"> • <code>show adoption info</code> - is the command. This command can also be used as: <p><code>show adoption info</code> The command can also be extended as: <code>show adoption info {on <DEVICE-NAME>}</code> here:</p> <ul style="list-style-type: none"> • <code>{on <DEVICE-NAME>}</code> - is the optional keyword.
<p>command / keyword</p>	<p>The first word is always a command. Keywords are words that must be entered as is. Commands and keywords are mandatory.</p> <p>For example, the command, <code>nx9500-6C8809>show wireless</code> is documented as: <code>show wireless</code> where:</p> <ul style="list-style-type: none"> • <code>show</code> - is the command • <code>wireless</code> - is the keyword
<p>()</p>	<p>Any command/keyword/variable or a combination of them inside a '(&)' pair are recursive. All recursive commands can be listed in any order and can be used once along with the rest of the commands.</p> <p>For example, the command, <code>crypto pki export request generate-rsa-key test autogen-subject-name ...</code> is documented as: <code>nx9500-6C8809#crypto pki export request generate-rsa-key test autogen-subject-name (<URL>,email <EMAIL>,fqdn <FQDN>,ip-address <IP>)</code> here:</p> <ul style="list-style-type: none"> • <code>crypto pki export request generate-rsa-key <RSA-KEYPAIR-NAME> auto-gen-subject-name</code> - is the command • <code><RSA-KEYPAIR-NAME></code> - is the RSA keypair name (in this example, the keypair name is 'test') • <code>(<URL>,email <EMAIL>,fqdn <FQDN>,ip-address <IP>)</code> - is the set of recursive parameters (separated by commas) that can be used in any order.



INTRODUCTION

INTRODUCTION

This chapter describes the commands available within a device's CLI (Command Line Interface) structure. CLI is available for wireless controller, access points (APs), and service platforms.

Access the CLI by using:

- A terminal emulation program running on a computer connected to the serial port on the device (AP, wireless controller, and service platform).
- A Telnet session through SSH (Secure Shell) over a network.

Configuration for connecting to a Controller using a terminal emulator

If connecting through the serial port, use the following settings to configure your terminal emulator:

<i>Bits Per Second</i>	19200 For AP 8533, AP 8432, AP 7622, AP 7632, AP 7622, AP 7612, AP 7602, AP 7562, AP 7532, AP 7522, AP 7502, AP 6562, AP 6522 model access points set this value to 115200.
<i>Data Bits</i>	8
<i>Parity</i>	None
<i>Stop Bit</i>	1
<i>Flow Control</i>	None

When a CLI session is established, complete the following (user input is in **bold**):

```
login as: <username>  
administrator's login password: <password>
```

User Credentials

Use the following credentials when logging into a device for the first time:

User Name	admin
Password	admin123

When logging into the CLI for the first time, you are prompted to change the password. Reset the password and use it for subsequent logins.

Examples in this reference guide

Examples used in this reference guide are generic to the each supported wireless controller, service platform, and AP model. Commands that are not common, are identified using the notation "Supported in the following platforms." For an example, see below:

Supported in the following platforms:

- Wireless Controller – RFS 4000

The above example indicates the command is only available for a RFS 4000 model wireless controller.

CLI Overview

The CLI is used for configuring, monitoring, and maintaining the network. The user interface allows you to execute commands on supported wireless controllers, service platforms, and APs, using either a serial console or a remote access method.

This chapter describes basic CLI features. Topics covered include an introduction to command modes, navigation and editing features, help features and command history.

The CLI is segregated into different command modes. Each mode has its own set of commands for configuration, maintenance, and monitoring. The commands available at any given time depend on the mode you are in, and to a lesser extent, the particular model used. Enter a question mark (?) at the system prompt to view a list of commands available for each command mode/instance.

Use specific commands to navigate from one command mode to another. The standard order is: USER EXEC mode, PRIV EXEC mode and GLOBAL CONFIG mode.

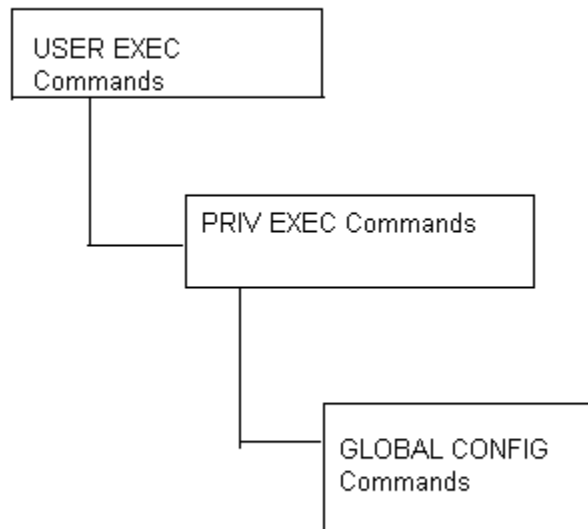


Figure: Hierarchy of User Modes

Command Modes

A session generally begins in the USER EXEC mode (one of the two access levels of the EXEC mode). For security, only a limited subset of EXEC commands are available in the USER EXEC mode. This level is reserved for tasks that do not change the device's (wireless controller, service platform, or AP) configuration.

```
rfs4000-6DB5D4>
```


The system prompt signifies the device name and the last three bytes of the device MAC address.

To access commands, enter the PRIV EXEC mode (the second access level for the EXEC mode). Once in the PRIV EXEC mode, enter any EXEC command. The PRIV EXEC mode is a superset of the USER EXEC mode.

```
rfs4000-6DB5D4>enable
rfs4000-6DB5D4#
```

Most of the USER EXEC mode commands are one-time commands and are not saved across device reboots. Save the command by executing 'commit' command. For example, the show command displays the current configuration and the clear command clears the interface.

Access the GLOBAL CONFIG mode from the PRIV EXEC mode. In the GLOBAL CONFIG mode, enter commands that set general system characteristics. Configuration modes, allow you to change the running configuration. If you save the configuration later, these commands are stored across device reboots.

Access a variety of protocol specific (or feature-specific) modes from the global configuration mode. The CLI hierarchy requires you to access specific configuration modes only through the global configuration mode.

```
rfs4000-6DB5D4#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
rfs4000-6DB5D4(config)#
```

You can also access sub-modes from the global configuration mode. Configuration sub-modes define specific features within the context of a configuration mode.

```
rfs4000-6DB5D4(config)#aaa-policy test
rfs4000-6DB5D4(config-aaa-policy-test)#
```

The following table summarizes the available controller commands:

Table 3: Controller CLI Modes and Commands

User Exec Mode	Priv Exec Mode	Global Configuration Mode
captive-portal-page-upload	archive	aaa-policy
change-passwd	boot	aaa-tacacs-policy
clear	captive-portal-page-upload	alias
clock	cd	AP 6522
cluster	change-passwd	AP 6562
commit	clear	AP 7502
connect	clock	AP 7522
create-cluster	cluster	AP 7532
crypto	commit	AP 7562
crypto-cmp-cert-update	configure	AP 7602
database	connect	AP 7612
database-backup	copy	AP 7622

Table 3: Controller CLI Modes and Commands (continued)

User Exec Mode	Priv Exec Mode	Global Configuration Mode
database-restore	cpe (supported on NX 7500, NX 9600 and VX 9000)	AP 7632
debug	create-cluster	AP 7662
device-upgrade	crypto	AP 8163
disable	crypto-cmp-cert-updated	AP 8432
enable	database	AP 8533
file-sync	database-backup	application
help	database-restore	application-group
join-cluster	debug	application-policy
l2tpv3	delete	
logging	device-upgrade	auto-provisioning-policy
mint	diff	bgp
no	dir	bonjour-gw-discovery-policy
on	disable	bonjour-gw-forwarding-policy
opendns	edit	bonjour-gw-query-forwarding-policy
page	enable	captive-portal
ping	erase	clear
ping6	factory-reset	client-identity
revert	file-sync	client-identity-group
service	halt	clone
show	help	crypto-cmp-policy
ssh	join-cluster	customize
telnet	l2tpv3	database-client-policy (supported only on VX 9000)
terminal	logging	database-policy (supported only on NX 9500, NX 9600, and VX 9000)
time-it	mint	device
traceroute	mkdir	device-categorization
traceroute6	more	dhcp-server-policy
virtual-machine (supported only on NX 9500, NX 96XX and VX 9000)	no	dhcp6-server-policy
watch	on	dns-whitelist
write	opendns	event-system-policy
clrscr	page	firewall-policy
exit	ping	global-association-list

Table 3: Controller CLI Modes and Commands (continued)

User Exec Mode	Priv Exec Mode	Global Configuration Mode
	ping6	guest-management
	pwd	help
	raid (supported only on NX 9500 and NX 7530)	host
	re-elect	igmp-snoop-policy (This command has been deprecated. IGMP snooping is now configurable under the profile/device configuration mode. For more information, see ip on page 1154.
	reload	inline-password-encryption
	remote-debug	ip
	rename	ipv6
	revert	ipv6-router-advertisement-policy
	rmdir	l2tpv3
	self	mac
	service	management-policy
	show	meshpoint
	ssh	meshpoint-qos-policy
	t5 (supported only on RFS 4000, NX 9600, and VX 9000)	mint-policy
	telnet	nac-list
	terminal	no
	time-it	nsight-policy
	traceroute	NX 5500 (supported only on NX 9600 and VX 9000)
	traceroute6	NX 7500 (supported only on NX 9600 and VX 9000)
	upgrade	NX 9000 (supported only on NX 9600 and VX 9000)
	upgrade-abort	NX 9600
	virtual-machine (supported only on NX 9600 and VX 9000)	passpoint-policy
	watch	password-encryption
	write	profile
	clrscr	radio-qos-policy
	exit	radius-group
		radius-server-policy

Table 3: Controller CLI Modes and Commands (continued)

User Exec Mode	Priv Exec Mode	Global Configuration Mode
		radius-user-pool-policy
		rename
		roaming-assist-policy
		role-policy
		route-map
		routing-policy
		rtl-server-policy
		schedule-policy
		self
		sensor-policy
		smart-rf-policy
		t5 (supported only on NX 7500, NX 9600 and VX 9000)
		url-filter (supported only on NX 9600 and VX 9000)
		url-list (supported only on NX 9600 and VX 9000)
		vx9000 (supported only on NX 9600 and VX 9000)
		web-filter-policy
		wips-policy
		wlan
		wlan-qos-policy
		write
		clrscr
		commit
		do
		end
		exit
		revert
		service
		show

Getting Context Sensitive Help

Enter a question mark (?) at the system prompt to display a list of commands available for each mode. Obtain a list of arguments and keywords for any command using the CLI context-sensitive help.

Use the following commands to obtain help specific to a command mode, command name, keyword or argument:

Command	Description
(prompt)# help	Displays a brief description of the help system
(prompt)# abbreviated-command-entry?	Lists commands in the current mode that begin with a particular character string
(prompt)# abbreviated-command-entry<Tab>	Completes a partial command name
(prompt)# ?	Lists all commands available in the command mode
(prompt)# command ?	Lists the available syntax options (arguments and keywords) for the command
(prompt)# command keyword ?	Lists the next available syntax option for the command



Note

The system prompt varies depending on the configuration mode.



Note

Enter Ctrl + V to use ? as a regular character and not as a character used for displaying context sensitive help. This is required when the user has to enter a URL that ends with a ?



Note

The escape character used through out the CLI is "\". To enter a "\" use "\\" instead.

When using context-sensitive help, the space (or lack of a space) before the question mark (?) is significant. To obtain a list of commands that begin with a particular sequence, enter the characters followed by a question mark (?). Do not include a space. This form of help is called word help, because it completes a word.

```
rfs4000-6DB5D4#service?
service Service Commands
rfs4000-6DB5D4#service
```

Enter a question mark (?) (in place of a keyword or argument) to list keywords or arguments. Include a space before the "?". This form of help is called command syntax help. It shows the keywords or arguments available based on the command/keyword and argument already entered.

```
rfs4000-6DB5D4#service ?
  block-adopter-config-update      Block configuration updates from the
  bluetooth                        Bluetooth service commands
  clear                             Clear adoption history
  cli-tables-skin                  Choose a formatting layout/skin for CLI
                                   tabular outputs (EXPERIMENTAL-Applies only
                                   to certain commands)
  cluster                          Cluster Protocol
  copy                             Copy files or directories
  delete                           Delete sessions
  delete-offline-aps               Delete Access Points that are configured
                                   but offline
  force-send-config                 Resend configuration to the device
  force-update-vm-stats             Force VM statistics to be pushed up to the
                                   NOC
```

load-balancing	Wireless load-balancing service commands
load-ssh-authorized-keys	Load Ssh authorized keys
locator	Enable leds flashing on the device
mint	MiNT protocol
pktpcap	Start packet capture
pm	Process Monitor
radio	Radio parameters
radius	Radius test
request-full-config-from-adopter	Request full configuration from the adopter
set	Set global options
show	Show running system information
signal	Send a signal to a process
smart-rf	Smart-RF Management Commands
snmp	Snmp
ssm	Command related to ssm
start-shell	Provide shell access
syslog	Syslog service
trace	Trace a process for system calls and signals
troubleshoot	Troubleshooting
wireless	Wireless commands

rfs4000-6DB5D4#

It is possible to abbreviate commands and keywords to allow a unique abbreviation. For example, "configure terminal" can be abbreviated as **conf t**. Since the abbreviated command is unique, the wireless controller accepts the abbreviation and executes the command.

Enter the help command (available in any command mode) to provide the following description:

```
rfs4000-6DB5D4>help
```

When using the CLI, help is provided at the command line when typing '?'. If no help is available, the help content will be empty. Backup until entering a '?' shows the help content.

There are two styles of help provided:

1. Full help. Available when entering a command argument (e.g. 'show ?'). This will describe each possible argument.
2. Partial help. Available when an abbreviated argument is entered. This will display which arguments match the input (e.g. 'show ve?').

```
rfs4000-6DB5D4>
```

Using the No Command

Almost every command has a **no** form. Use **no** to disable a feature or function or return it to its default. Use the command without the **no** keyword to re-enable a disabled feature.

Basic Conventions

Keep the following conventions in mind while working within the CLI structure:

- Use ? at the end of a command to display available sub-modes. Type the first few characters of the sub-mode and press the tab key to add the sub-mode. Continue using ? until you reach the last sub-mode.
- Pre-defined CLI commands and keywords are case-insensitive: `cfg` = `Cfg` = `CFG`. However (for clarity), CLI commands and keywords are displayed (in this guide) using mixed case. For example, `apPolicy`, `trapHosts`, `channellInfo`.

- Enter commands in uppercase, lowercase, or mixed case. Only passwords are case sensitive.

Using CLI Editing Features and Shortcuts

A variety of shortcuts and edit features are available. The following sections describe these features:

- [Moving the Cursor on the Command Line](#)
- [Completing a Partial Command Name](#)
- [Command Output pagination](#)

Moving the Cursor on the Command Line

The following table shows the key combinations or sequences to move the command line cursor. **Ctrl** defines the control key, which must be pressed simultaneously with its associated letter key. **Esc** means the escape key (which must be pressed first), followed by its associated letter key. Keys are not case sensitive. Specific letters are used to provide an easy way of remembering their functions. The bold characters indicate the relation between a letter and its function.

Table: Keystrokes Details

Keystrokes	Function Summary	Function Details
Left Arrow or Ctrl-B	Back character	Moves the cursor one character to the left When entering a command that extends beyond a single line, press the Left Arrow or Ctrl-B keys repeatedly to move back to the system prompt.
Right Arrow or Ctrl-F	Forward character	Moves the cursor one character to the right
Esc- B	Back word	Moves the cursor back one word
Esc- F	Forward word	Moves the cursor forward one word
Ctrl-A	Beginning of line	Moves the cursor to the beginning of the command line
Ctrl-E	End of line	Moves the cursor to the end of the command line
Ctrl-D		Deletes the current character
Ctrl-U		Deletes text up to cursor
Ctrl-K		Deletes from the cursor to end of the line
Ctrl-P		Obtains the prior command from memory
Ctrl-N		Obtains the next command from memory
Esc-C		Converts the letter at the cursor to uppercase
Esc-L		Converts the letter at the cursor to lowercase
Esc-D		Deletes the remainder of a word
Ctrl-W		Deletes the word up to the cursor
Ctrl-Z		Returns to the root prompt
Ctrl-T		Transposes the character to the left of the cursor with the character located at the cursor
Ctrl-L		Clears the screen

Completing a Partial Command Name

If you cannot remember a command name (or if you want to reduce the amount of typing you have to perform), enter the first few letters of a command, then press the Tab key. The command line parser completes the command if the string entered is unique to the command mode. If your keyboard does not have a **Tab** key, press **Ctrl-L**.

The CLI recognizes a command once you have entered enough characters to make the command unique. If you enter "conf" within the privileged EXEC mode, the CLI associates the entry with the configure command, since only the configure command begins with **conf**.

In the following example, the CLI recognizes a unique string in the privileged EXEC mode when the Tab key is pressed:

```
rfs4000-6DB5D4#conf[TAB]
rfs4000-6DB5D4#configure
```

When using the command completion feature, the CLI displays the full command name. The command is not executed until the **Return** or **Enter** key is pressed. Modify the command if the full command was not what you intended in the abbreviation. If entering a set of characters (indicating more than one command), the system lists all commands beginning with that set of characters.

Enter a question mark (?) to obtain a list of commands beginning with that set of characters. Do not leave a space between the last letter and the question mark (?).

In the following example, all commands, available in the current context, starting with the characters 'co' are listed:

```
rfs4000-6DB5D44#co?
  commit      Commit all changes made in this session
  configure   Enter configuration mode
  connect     Open a console connection to a remote device
  copy        Copy from one file to another

rfs4000-6DB5D4#
```



Note

The characters entered before the question mark are reprinted to the screen to complete the command entry.

Command Output pagination

Output often extends beyond the visible screen length. For cases where output continues beyond the screen, the output is paused and a

```
--More--
```

prompt displays at the bottom of the screen. To resume the output, press the Enter key to scroll down one line or press the **Space bar** to display the next full screen of output.

Creating Profiles

Profiles are sort of a 'template' representation of configuration. The system has:

- a default profile for each of the following wireless controllers:
 - RFS 4000
- a default profile for each of the following service platforms:

- NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000
- a default profile for each of the following access points:
 - AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533

You can modify a default profile. In the following example, an IP address is assigned to the management port on the default RFS 4000 profile.

```
rfs4000-6DB5D4(config)#profile rfs4000 default-rfs4000
rfs4000-6DB5D4(config-profile-default-rfs4000)#interface me1
rfs4000-6DB5D4(config-profile-default-rfs4000-if-me1)#ip address 172.16.10.2/24
rfs4000-6DB5D4(config-profile-default-rfs4000-if-me1)#commit
rfs4000-6DB5D4(config-profile-default-rfs4000)#exit
rfs4000-6DB5D4(config)#
```

The following command displays a default AP 7562 profile configuration:

```
rfs4000-6DB5D4(config-profile-default-ap7562)#
rfs4000-6DB5D4(config-profile-default-ap7562)#show context
profile ap7562 default-ap7562
  autoinstall configuration
  autoinstall firmware
  crypto ikev1 policy ikev1-default
    isakmp-proposal default encryption aes-256 group 2 hash sha
  crypto ikev2 policy ikev2-default
    isakmp-proposal default encryption aes-256 group 2 hash sha
  crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
  crypto ikev1 remote-vpn
  crypto ikev2 remote-vpn
  crypto auto-ipsec-secure
  crypto load-management
  crypto remote-vpn-client
  interface radiol
    placement outdoor
  interface radio2
    placement outdoor
  interface ge1
  interface ge2
  interface vlan1
    ip address dhcp
    ip address zeroconf secondary
    ip dhcp client request options all
--More--
rfs4000-6DB5D4(config-profile-default-ap7562)#
```

Change the default profile by creating vlan 150 and mapping to ge3 Physical interface

Log on to the controller in config mode and follow the procedure below:

```
rfs4000-6DB5D4(config-profile-default-rfs4000)# interface vlan 150
rfs4000-6DB5D4(config-profile-default-rfs4000-if-vlan150)# ip address 192.168.150.20/24
rfs4000-6DB5D4(config-profile-default-rfs4000-if-vlan150)# exit
rfs4000-6DB5D4(config-profile-default-rfs4000)# interface ge 3
rfs4000-6DB5D4(config-profile-default-rfs4000-if-ge3)# switchport access vlan 150
rfs4000-6DB5D4(config-profile-default-rfs4000-if-ge3)# commit write
[OK]
rfs4000-6DB5D4(config-profile-default-rfs4000-if-ge3)#show interface vlan 150
Interface vlan150 is UP
  Hardware-type: vlan, Mode: Layer 3, Address: 00-15-70-81-70-1D
  Index: 6, Metric: 1, MTU: 1500
  IP-Address: 192.168.150.20/24
    input packets 0, bytes 0, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
```

```

output packets 2, bytes 140, dropped 0
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
collisions 0
IPv6 mode is disabled

```

```
rfs4000-6DB5D4(config-profile-default-rfs4000-if-ge3)#
```

Viewing Configured APs

To view previously configured APs, enter the following command:

```
rfs4000-6DB5D4>show wireless ap configured
```

```

-----
IDX      NAME          MAC          PROFILE      RF-DOMAIN    ADOPTED-BY
-----
 1 ap7522-8330A4 84-24-8D-83-30-A4 default-ap7522 default      00-15-70-81-74-2D
 2 ap8533-9A12DB 74-67-F7-9A-12-DB default-ap8533 default      un-adopted
 3 ap7562-84A224 84-24-8D-84-A2-24 default-ap7562 TechPubs    00-15-70-81-74-2D
-----
rfs4000-6DB5D4>

```

Enabling Remote Administration

A terminal server may function in remote administration mode if either the terminal services role is not installed on the machine or the client used to invoke the session has enabled the admin controller.

- A terminal emulation program running on a computer connected to the serial port on the controller. The serial port is located on the front of the controller.
- A Telnet session through a SSH (Secure Shell) over a network. The Telnet session may or may not use SSH depending on how the controller is configured. Using SSH for remote administration tasks is recommended.

Configuring Telnet for Management Access

To enable Telnet for management access, use the serial console to login to the device and perform the following:

- 1 The session, by default, opens in the USER EXEC mode (one of the two access levels of the EXEC mode). Access the PRIV EXEC mode from the USER EXEC mode.

```
rfs4000-6DB5D4>en
rfs4000-6DB5D4#>
```

- 2 Access the GLOBAL CONFIG mode from the PRIV EXEC mode.

```
rfs4000-6DB5D4>en
rfs4000-6DB5D4#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
rfs4000-6DB5D4(config)#
```

- 3 Go to 'default-management-policy' mode.

```
rfs4000-6DB5D4(config)#management-policy ?
MANAGEMENT Name of the management policy to be configured (will be created
if it does not exist)
```

```
rfs4000-6DB5D4(config)#management-policy default
rfs4000-6DB5D4(config-management-policy-default)#
```

- 4 Enter Telnet and the port number at the command prompt. Note, the port number is optional. If you do not specify the port, the system, by default, assigns port 23 for Telnet. Commit your changes. Telnet is enabled.

```
rfs4000-6DB5D4(config-management-policy-default)#telnet
rfs4000-6DB5D4(config-management-policy-default)#commit write
```

```
rfs4000-6DB5D4(config-management-policy-default)#end
rfs4000-6DB5D4#exit
```

- 5 Connect to the controller through Telnet using its configured IP address. If logging in for the first time, use the following credentials:

User Name	admin
Password	admin123 Note: When logging in for the first time, you will be prompted to change the password. Re-set the password and use it for subsequent logins.

- 6 To change password, on subsequent logins, access the default management-policy configuration mode and enter the username, new password, role, and access details.

```
rfs4000-6DB5D4(config-management-policy-default)#user testuser password test@123
role helpdesk access all
rfs4000-6DB5D4(config-management-policy-default)#commit
rfs4000-6DB5D4(config-management-policy-default)#show context
management-policy default
telnet
http server
https server
no ftp
ssh
user admin password 1 fd07f19c6caf46e5b7963a802d422a708ad39a24906e04667c8642299c8462f1
role superuser access all
user testuser password 1
32472f01757293a181738674bdf068ffe0b777ce145524fc669278820ab582c0 role helpdesk access
all
snmp-server community 2 uktRccdr9eLoByF5PCSuFAAAAAeB78WhgTbSKDi96msyUiW+ rw
snmp-server community 2 Ne+R15zlwEdhybKxfgb6JwAAAAZzvrLGzU/xWXgwFtwF5JdD ro
snmp-server user snmptrap v3 encrypted des auth md5 2 WUTBNiUi7tL4ZbU2I7Eh/
QAAAAiDhBZTln0UIu+y/W6E/0tR
snmp-server user snmpmanager v3 encrypted des auth md5 2 9Fva4fYV1WL4ZbU2I7Eh/
QAAAAjdvbWANBNw+We/xHkH9kLi
no https use-secure-ciphers-only
rfs4000-6DB5D4(config-management-policy-default)#
```

- 7 Log on to the Telnet console and provide the user details configured in the previous step to access the controller.

```
rfs4000 release 5.9.2.0-015D
rfs4000-6DB5D4 login: testuser
Password:
Welcome to CLI
Starting CLI...rfs4000-6DB5D4>
```

Configuring SSH for Management Access

By default, SSH is enabled from the factory settings on the controller. The controller requires an IP address and login credentials.

To enable SSH access on a device, login through the serial console and perform the following:

- 1 The session, by default, opens in the USER EXEC mode (one of the two access levels of the EXEC mode). Access the PRIV EXEC mode from the USER EXEC mode.

```
rfs4000-6DB5D4>en
rfs4000-6DB5D4#
```

- 2 Access the GLOBAL CONFIG mode from the PRIV EXEC mode.

```
rfs4000-6DB5D4>en
rfs4000-6DB5D4#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.
 rfs4000-6DB5D4(config)#

- Go to 'default-management-policy' mode.

```
rfs4000-6DB5D4(config)#management-policy ?
  MANAGEMENT Name of the management policy to be configured (will be created
                if it does not exist)
```

```
rfs4000-6DB5D4(config)#management-policy default
rfs4000-6DB5D4(config-management-policy-default)#
```

- Enter SSH at the command prompt.

```
rfs4000-6DB5D4(config-management-policy-default)#ssh
rfs4000-6DB5D4(config-management-policy-default)#commit write
rfs4000-6DB5D4(config-management-policy-default)#end
rfs4000-6DB5D4#exit
```

- Connect to the controller through SSH using its configured IP address. If logging in for the first time, use the following credentials:

User Name	admin
Password	admin123
	Note: When logging in for the first time, you will be prompted to change the password. Re-set the password and use it for subsequent logins.

- On subsequent logins, to change the password, access the default management-policy configuration mode and enter the username, new password, role, and access details.

```
rfs4000-6DB5D4(config-management-policy-default)#user testuser password test@123
  role helpdesk access all
rfs4000-6DB5D4(config-management-policy-default)#commit
rfs4000-6DB5D4(config-management-policy-default)#show context
management-policy default
  telnet
  http server
  https server
  no ftp
  ssh
  user admin password 1 fd07f19c6caf46e5b7963a802d422a708ad39a24906e04667c8642299c8462f1
  role superuser access all
  user testuser password 1
32472f01757293a181738674bdf068ffe0b777ce145524fc669278820ab582c0 role helpdesk access
all
  snmp-server community 2 uktRccdr9eLoByF5PCSuFAAAAAeB78WhgTbSKDi96msyUiW+ rw
  snmp-server community 2 Ne+R15zlwEdhybKxfbd6JwAAAAZzvrLGzU/xWXgwFtwF5JdD ro
  snmp-server user snmptrap v3 encrypted des auth md5 2 WUTBNiUi7tL4ZbU2I7Eh/
QAAAAiDhBZTln0UIu+y/W6E/0tr
  snmp-server user snmpmanager v3 encrypted des auth md5 2 9Fva4fYV1WL4ZbU2I7Eh/
QAAAAjdvbWANBNw+We/xHkH9kLi
  no https use-secure-ciphers-only
rfs4000-6DB5D4(config-management-policy-default)#
```

- Log on to the SSH console and provide the user details configured in the previous step to access the controller.

```
rfs4000 release 5.9.2.0-015D
rfs4000-6DB5D4 login: testuser
Password:
Welcome to CLI
Starting CLI...
rfs4000-6DB5D4>
```

USER EXEC MODE COMMANDS

USER EXEC MODE COMMANDS

Logging in to the wireless controller places you within the USER EXEC command mode. Typically, a login requires a user name and password. You have three login attempts before the connection attempt is refused. USER EXEC commands (available at the user level) are a subset of the commands available at the privileged level. In general, USER EXEC commands allow you to connect to remote devices, perform basic tests, and list system information.

To list available USER EXEC commands, use ? at the command prompt. The USER EXEC prompt consists of the device host name followed by an angle bracket (>).

```
<DEVICE>>?
```

```
Command commands:
```

```
  captive-portal-page-upload  Captive portal internal and advanced page upload
  change-passwd               Change password
  clear                       Clear
  clock                       Configure software system clock
  cluster                    Cluster commands
  commit                     Commit all changes made in this session
  connect                    Open a console connection to a remote device
  create-cluster             Create a cluster
  crypto                     Encryption related commands
  crypto-cmp-cert-update     Update the cmp certs
  database                   Database
  database-backup            Backup database
  database-restore          Restore database
  debug                     Debugging functions
  device-upgrade            Device firmware upgrade
  disable                   Turn off privileged mode command
  enable                    Turn on privileged mode command
  file-sync                 File sync between controller and adoptees
  help                      Description of the interactive help system
  join-cluster              Join the cluster
  l2tpv3                    L2tpv3 protocol
  logging                   Modify message logging facilities
  mint                      MiNT protocol
  no                        Negate a command or set its defaults
  on                        On RF-Domain
 .opendns                   OpenDNS configuration
  page                      Toggle paging
  ping                      Send ICMP echo messages
  ping6                     Send ICMPv6 echo messages
  revert                    Revert changes
  service                   Service Commands
  show                      Show running system information
  ssh                       Open an ssh connection
  telnet                    Open a telnet connection
  terminal                  Set terminal line parameters
  time-it                   Check how long a particular command took between
                           request and completion of response
  traceroute                Trace route to destination
  traceroute6               Trace route to destination(IPv6)
  virtual-machine           Virtual Machine
  watch                     Repeat the specific CLI command at a periodic
                           interval
  write                     Write running configuration to memory or
```

```

terminal
clrscr          Clears the display screen
exit           Exit from the CLI

<DEVICE>>

```

user-exec-commands

The following table summarizes the User Exec Configuration Mode commands:

Table 4: User Exec Mode Commands

Command	Description
captive-portal-page-upload (user and privi exec modes) on page 27	Uploads captive portal advanced pages
change-passwd (user and privi exec modes) on page 31	Changes the password of a logged user
clear (user and privi exec modes) on page 32	Resets the last saved command
clock (user and privi exec modes) on page 44	Configures the system clock
cluster (user and privi exec modes) on page 46	Accesses the cluster context
connect (user and privi exec modes) on page 46	Establishes a console connection to a remote device
create-cluster (user and privi exec modes) on page 47	Creates a new cluster on a specified device
crypto (user and privi exec modes) on page 49	Enables encryption
crypto-cmp-cert-policy (user and privi exec modes) on page 58	Triggers a CMP certificate update on a specified device or devices
database (user and privi exec modes) on page 59	Enables automatic repairing (vacuuming) and dropping of databases (Captive-portal and NSight)
database-backup (user and privi exec modes) on page 63	Backs up captive-portal and/or NSight database to a specified location and file on an FTP or SFTP server
database-restore (user and privi exec modes) on page 64	Restores a previously exported database [captive-portal and/or NSight]. Previously exported databases (backed up to a specified FTP or SFTP server) are restored to the original database.
device-upgrade (user and privi exec modes) on page 65	Configures device firmware upgrade settings
disable on page 73	Turns off (disables) the privileged mode command set
enable on page 73	Turns on (enables) the privileged mode command set
join-cluster (user and privi exec modes) on page 77	Adds a device (Access Point, wireless controller, or service platform) to an existing cluster of devices
file-sync (user and privi exec modes) on page 74	Configures parameters enabling syncing of PKCS#12 and wireless-bridge certificate between the staging-controller and adopted access points
l2tpv3 (user and privi exec modes) on page 79	Establishes or brings down L2TPv3 (Layer 2 Tunneling Protocol Version 3) tunnels
logging (user and privi exec modes) on page 80	Modifies message logging facilities

Table 4: User Exec Mode Commands (continued)

Command	Description
mint (user and privi exec modes) on page 82	Configures MiNT protocol
no (user exec mode) on page 83	Negates a command or sets its default
opendns (user and privi exec modes) on page 86	Connects to the OpenDNS site using OpenDNS registered credentials (username, password) OR OpenDNS API token to fetch the OpenDNS device_id. This command is a part of the process integrating access points, controllers, and service platforms with OpenDNS.
page (user and privi exec modes) on page 89	Toggles a device's (Access Point, wireless controller, or service platform) paging function
ping (user and privi exec modes) on page 90	Sends ICMP echo messages to a user-specified location
ping6 (user and privi exec modes) on page 91	Sends ICMPv6 echo messages to a user-specified location
ssh (user and privi exec modes) on page 93	Opens an SSH connection between two network devices
telnet (user and privi exec modes) on page 94	Opens a Telnet session
terminal (user and privi exec modes) on page 95	Sets the length and width of the terminal window
time-it (user and privi exec modes) on page 96	Verifies the time taken by a particular command between request and response
traceroute (user-privi-exec-mode) on page 96	Traces the route to its defined IPv4 destination
traceroute6 (user-privi-exec-mode) on page 97	Traces the route to its defined IPv6 destination
watch on page 104	Repeats a specific CLI command at a periodic interval
virtual-machine	Installs, configures, and monitors the status of VMs (<i>virtual machines</i>). This command is specific to the NX 9500 and NX 9510 series service platforms.
exit (user exec mode) on page 103	Ends the current CLI session and closes the session window



Note

For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see [COMMON COMMANDS](#) on page 640.



Note

The input parameter <HOSTNAME>, if used in syntaxes across this chapter, cannot include an underscore (_) character.

captive-portal-page-upload (user and privi exec modes)

Uploads captive portal advanced pages to adopted access points. Use this command to provide access points with specific captive portal configurations, so that they can successfully provision login,

welcome, and condition pages to clients attempting to access the wireless network using the captive portal.



Note

Ensure that the captive portal pages to upload are *.tar files.



Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
captive-portal-page-upload [<CAPTIVE-PORTAL-NAME> |cancel-upload|delete-file|load-file]
captive-portal-page-upload <CAPTIVE-PORTAL-NAME> [<MAC/HOSTNAME> |all|rf-domain]
captive-portal-page-upload <CAPTIVE-PORTAL-NAME> [<MAC/HOSTNAME> |all] {upload-time <TIME>}
captive-portal-page-upload <CAPTIVE-PORTAL-NAME> rf-domain [<DOMAIN-NAME> |all]
{from-controller} {(upload-time <TIME>)}
captive-portal-page-upload cancel-upload [<MAC/HOSTNAME> |all|on rf-domain [<DOMAIN-NAME> |
all]]
captive-portal-page-upload delete-file <CAPTIVE-PORTAL-NAME> <FILE-NAME>
captive-portal-page-upload load-file <CAPTIVE-PORTAL-NAME> <URL>
```

Parameters

```
captive-portal-page-upload <CAPTIVE-PORTAL-NAME> [<MAC/HOSTNAME> |all] {upload-time <TIME>}
```

captive-portal-page-upload <CAPTIVE-PORTAL-NAME>	Uploads advanced pages of the captive portal identified by the <CAPTIVE-PORTAL-NAME> parameter <ul style="list-style-type: none">• <CAPTIVE-PORTAL-NAME> - Specify captive portal's name (should be existing and configured).
<MAC/HOSTNAME>	Uploads to a specified AP <ul style="list-style-type: none">• <MAC/HOSTNAME> - Specify the AP's MAC address or hostname.
all	Uploads to all APs
upload-time <TIME>	Schedules an AP upload time <ul style="list-style-type: none">• <TIME> - Specify upload time in the MM/DD/YYYY-HH:MM or HH:MM format. The scheduled upload time is your local system's time. It is not the access point, controller, service platform, or virtual controller time and it is not synched with the device. To view a list of uploaded captive portal files, execute the show > captive-portal-page-upload > list-files <CAPTIVE-PORTAL-NAME> command.

```
captive-portal-page-upload <CAPTIVE-PORTAL-NAME> rf-domain [<DOMAIN-NAME> |all]
{from-controller} {(upload-time <TIME>)}
```


captive-portal-page-upload <CAPTIVE-PORTAL-NAME>	Uploads advanced pages of the captive portal identified by the <CAPTIVE-PORTAL-NAME> parameter <ul style="list-style-type: none"> • <CAPTIVE-PORTAL-NAME> – Specify the captive portal’s name (should be existing and configured).
rf-domain [<DOMAIN-NAME> all]	Uploads to all APs within a specified RF Domain or all RF Domains <ul style="list-style-type: none"> • <DOMAIN-NAME> – Uploads to APs within a specified RF Domain. Specify the RF Domain name. • all – Uploads to APs across all RF Domains
from-controller	Optional. Uploads captive-portal pages to APs via the controller to which the APs are adopted
upload-time <TIME>	Schedules an AP upload time <ul style="list-style-type: none"> • <TIME> – Specify upload time in the MM/DD/YYYY-HH:MM or HH:MM format. <p>The scheduled upload time is your local system’s time. It is not the access point, controller, service platform, or virtual controller time and it is not synched with the device.</p> <p>To view a list of uploaded captive portal files, execute the show > captive-portal-page-upload > list-files <CAPTIVE-PORTAL-NAME> command.</p>

```
captive-portal-page-upload cancel-upload [<MAC/HOSTNAME>|all|on rf-domain [<DOMAIN-NAME>|all]]
```

captive-portal-page-upload cancel-upload	Cancels a scheduled AP upload
cancel-upload [<MAC/HOSTNAME> all on rf-domain [<DOMAIN-NAME> all]]	Select one of the following options: <ul style="list-style-type: none"> • <MAC/HOSTNAME> – Cancels scheduled upload to a specified AP. Specify the AP’s MAC address or hostname. • all – Cancels all scheduled AP uploads • on rf- domain – Cancels all scheduled uploads within a specified RF Domain or all RF Domains <ul style="list-style-type: none"> • <DOMAIN-NAME> – Cancels scheduled uploads within a specified RF Domain. Specify the RF Domain name. • all – Cancels scheduled uploads across all RF Domains

```
captive-portal-page-upload delete-file <CAPTIVE-PORTAL-NAME> <FILE-NAME>
```

captive-portal-page-upload delete-file	Deletes a specified captive portal’s uploaded captive-portal Web page files
<CAPTIVE-PORTAL-NAME> <FILE-NAME>	Identifies the captive-portal and Web pages to delete <ul style="list-style-type: none"> • <CAPTIVE-PORTAL-NAME> – Specify the captive portal name. • <FILE-NAME> – Specify the file name. The specified internal captive portal page is deleted.

```
captive-portal-page-upload load-file <CAPTIVE-PORTAL-NAME> <URL>
```

captive-portal-page-upload load-file	Loads captive-portal advanced pages
<CAPTIVE-PORTAL-NAME> <URL>	<p>Specify the captive portal's name and location. The captive portal should be existing and configured.</p> <p>IPv4 URLs:</p> <ul style="list-style-type: none"> • tftp://<hostname IP>[:port]/path/file • ftp://<user>:<passwd>@<hostname IP>[:port]/path/file • sftp://<user>:<passwd>@<hostname IP>[:port]/path/file • http://<hostname IP>[:port]/path/file • cf:/path/file • usb<n>:/path/file <p>IPv6 URLs:</p> <ul style="list-style-type: none"> • tftp://<hostname IPv6>[:port]/path/file • ftp://<user>:<passwd>@<hostname IPv6>[:port]/path/file • sftp://<user>:<passwd>@<hostname IPv6>[:port]/path/file • http://<hostname IPv6>[:port]/path/file <p>Note: The captive portal pages are downloaded to the controller from the location specified here. After downloading use the captive-portal-page-upload > <CAPTIVE-PORTAL-NAME> > <DEVICE-OR-DOMAIN-NAME> command to upload these pages to APs.</p>

Examples (User Executable Mode)

```
ap6562-B1A214>captive-portal-page-upload load-file captive_portal_test tftp://89.89.89.17/
pages_new_only.tar
ap6562-B1A214>
ap6562-B1A214>show captive-portal-page-upload load-image-status
Download of captive_portal_test advanced page file is complete
ap6562-B1A214>
ap6562-B1A214>captive-portal-page-upload captive_portal_test all
-----
CONTROLLER          STATUS          MESSAGE
-----
FC-0A-81-B1-A2-14   Success        Added 6 APs to upload queue
-----
ap6562-B1A214>
ap6562-B1A214>show captive-portal-page-upload status
Number of APs currently being uploaded : 1
Number of APs waiting in queue to be uploaded : 0
-----
AP          STATE      UPLOAD TIME  PROGRESS  RETRIES  LAST UPLOAD  ERROR  UPLOADED BY
-----
ap6562-B1A738  downloading  immediate    100       0        -           None
-----
ap6562-B1A214>
```

Examples (Privilege Executable Mode)

```
ap6562-B1A214# captive-portal-page-upload load-file captive_portal_test tftp://89.89.89.17/
pages_new_only.tar
ap6562-B1A214#
ap6562-B1A214# show captive-portal-page-upload load-image-status
Download of captive_portal_test advanced page file is complete
ap6562-B1A214#
ap6562-B1A214# captive-portal-page-upload captive_portal_test all
-----
CONTROLLER          STATUS          MESSAGE
-----
```

```

-----
FC-0A-81-B1-A2-14          Success          Added 6 APs to upload queue
-----
ap6562-B1A214#
ap6562-B1A214@#show captive-portal-page-upload status
Number of APs currently being uploaded : 1
Number of APs waiting in queue to be uploaded : 0
-----
      AP          STATE      UPLOAD TIME  PROGRESS  RETRIES  LAST UPLOAD  ERROR  UPLOADED BY
-----
ap6562-B1A738  downloading  immediate   100      0        -            None
-----
ap6562-B1A214#

```

The following example lists captive portal CP-BW uploaded files:

```

nx7500-7F2C13#show captive-portal-page-upload list-files CP-BW
-----
      NAME          SIZE          LAST MODIFIED
-----
CP-BW-1.tar.gz    6133         2017-05-16 10:38:40
CP-BW.tar.gz      3370         2017-05-16 10:45:44
-----
nx7500-7F2C13#

```

change-passwd (user and privi exec modes)

Changes the password of a logged user. When this command is executed without any parameters, the password can be changed interactively.



Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
change-passwd {<OLD-PASSWORD>} <NEW-PASSWORD>
```

Parameters

```
change passwd {<OLD-PASSWORD>} <NEW-PASSWORD>
```

<OLD-PASSWORD>	Optional. Specify the existing password.
<NEW-PASSWORD>	Specify the new password.
Note: The password can also be changed interactively. To do so, press [Enter] after the command.	

Usage Guidelines

A password must be from 1 - 64 characters.

Examples (User Executable Mode)

```
rfs4000-6DB5D4>change-passwd
Enter old password:
Enter new password:
Password for user 'admin' changed successfully
Please write this password change to memory(write memory) to be persistent.
rfs4000-6DB5D4#write memory
OK
rfs4000-6DB5D4>
```

Examples (Privilege Executable Mode)

```
nx9500-6C8809#change-passwd
Enter old password:
Enter new password:
Password for user 'admin' changed successfully
Please write this password change to memory(write memory) to be persistent.
nx9500-6C8809#write memory
OK
nx9500-6C8809#
```

clear (user and privi exec modes)

Clears parameters, cache entries, table entries, and other similar entries. The clear command is available for specific commands only. The information cleared, using this command, depends on the mode in which the clear command is executed.



Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
clear [arp-cache|bonjour|cdp|counters|crypto|eguest|event-history|gre|ip|ipv6|lACP|lldp|
mac-address-table|mint|role|rtls|spanning-tree|traffic-shape|vrrp]
clear arp-cache {on <DEVICE-NAME>}
clear bonjour cache {on <DEVICE-NAME>}
clear [cdp|lldp] neighbors {on <DEVICE-NAME>}
clear counters [ap|radio|wireless-client]
clear counters [ap {<MAC>}|radio {<MAC/DEVICE-NAME>} {<1-3>}|wireless-client {<MAC>}] {(on
<DEVICE-OR-DOMAIN-NAME>)}
clear crypto [ike|ipsec] sa
clear crypto ike sa [<IP>|all] {on <DEVICE-NAME>}
clear crypto ipsec sa {on <DEVICE-NAME>}
clear event-history
clear gre stats {on <DEVICE-NAME>}
clear ip [bgp|dhcp|ospf]
clear ip [bgp|dhcp|ospf]
clear ip bgp [<IP>|all|external|process]
clear ip bgp [<IP>|all|external] {in/on/out/soft}
clear ip bgp [<IP>|all|external] {in prefix-filter} {on <DEVICE-NAME>}
clear ip bgp [<IP>|all|external] {out} {(on <DEVICE-NAME>)}
clear ip bgp [<IP>|all|external] {soft {in/out}} {on <DEVICE-NAME>}
clear ip bgp process {on <DEVICE-NAME>}
clear ip dhcp bindings [<IP>|all] {on <DEVICE-NAME>}
clear ip ospf process {on <DEVICE-NAME>}
clear mac-address-table {address|interface|vlan} {on <DEVICE-NAME>}
clear ipv6 neighbor-cache {on <DEVICE-NAME>}
clear lACP [<1-4> counters|counters]
clear mac-address-table {address <MAC>/vlan <1-4094>} {on <DEVICE-NAME>}
clear mac-address-table {address|interface|mac-auth-state|vlan} {on <DEVICE-NAME>}
clear mac-address-table {address <MAC>/vlan <1-4094>} {on <DEVICE-NAME>}
clear mac-address-table {interface [<IN-NAME>|ge <1-2>|port-channel <1-2>| vmif <1-8>]}
{on <DEVICE-NAME>}
clear mac-address-table mac-auth-state address <MAC> vlan <1-4094> {on <DEVICE-NAME>}
clear mint mlcp history {on <DEVICE-NAME>}
clear role ldap-stats {on <DEVICE-NAME>}
clear rtls [aer scout|ekahau]
clear rtls [aer scout|ekahau] {<MAC/DEVICE-NAME> {on <DEVICE-OR-DOMAIN-NAME>}}/on <DEVICE-
OR-DOMAIN-NAME>}
clear spanning-tree detected-protocols{interface/on}
clear spanning-tree detected-protocols {on <DEVICE-NAME>}
clear spanning-tree detected-protocols {interface [<INTERFACE-NAME>|ge <1-X>|me1|port-
channel <1-X>|pppoe1/up1/vlan <1-4094>|wwan1]} {on <DEVICE-NAME>}
clear traffic-shape statistics class <1-4> {(on <DEVICE-NAME>)}
clear vrrp [error-stats|stats] {on <DEVICE-NAME>}
```

Parameters

```
clear arp-cache {on <DEVICE-NAME>}
```

arp-cache	Clears ARP (Address Resolution Protocol) cache entries on a AP, wireless controller, or service platform. This protocol matches the layer 3 IP addresses to the layer 2 MAC addresses.
on <DEVICE-NAME>	Optional. Clears ARP cache entries on a specified device <ul style="list-style-type: none"><DEVICE-NAME> - Specify the name of the AP, wireless controller, or service platform.

```
clear bonjour cache {on <DEVICE-NAME>}
```

bonjour cache	Clears all Bonjour cached statistics. Once cleared the system has to re-discover available Bonjour services.
on <DEVICE-NAME>	Optional. Clears all Bonjour cached statistics on a specified device <ul style="list-style-type: none"> • <DEVICE-NAME> - Specify the name of the AP, wireless controller, or service platform.

```
clear [cdp|lldp] neighbors {on <DEVICE-NAME>}
```

cdp	Clears CDP (Cisco Discovery Protocol) (CDP) table entries
lldp	Clears LLDP (Link Layer Discovery Protocol) table entries
neighbors	Clears CDP or LLDP neighbor table entries based on the option selected in the preceding step
on <DEVICE-NAME>	Optional. Clears CDP or LLDP neighbor table entries on a specified device <ul style="list-style-type: none"> • <DEVICE-NAME> - Specify the name of the AP, wireless controller, or service platform.

```
clear counters [ap {<MAC>}|radio {<MAC/DEVICE-NAME>} {<1-X>}|wireless-client {<MAC>}] {(on <DEVICE-OR-DOMAIN-NAME>)}
```

counters	Clears counters based on the parameters passed. The options are: AP, radio, and wireless clients.
ap <MAC>	Clears counters for all APs or a specified AP <ul style="list-style-type: none"> • <MAC> - Optional. Specify the AP's MAC address. <p>Note: If no MAC address is specified, all AP counters are cleared.</p>
radio <MAC/DEVICE-NAME> <1-X>	Clears radio interface counters on a specified device or on all devices <ul style="list-style-type: none"> • <MAC/DEVICE-NAME> - Optional. Specify the device's hostname or MAC address. Optionally, append the radio interface number (to the radio ID) using one of the following formats: AA-BB-CC-DD-EE-FF:RX or HOSTNAME:RX (where RX is the interface number). • <1-X> - Optional. Identifies the radio interface by its index. Specify the radio interface index, if not specified as part of the radio ID. Note, the number of radio interfaces available varies with the access point type. <p>Note: If no device name or MAC address is specified, all radio interface counters are cleared.</p>
wireless-client <MAC>	Clears counters for all wireless clients or a specified wireless client <ul style="list-style-type: none"> • <MAC> - Optional. Specify the wireless client's MAC address. <p>Note: If no MAC address is specified, all wireless client counters are cleared.</p>
on <DEVICE-OR-DOMAIN-NAME>	The following option is common to all of the above keywords: <ul style="list-style-type: none"> • on <DEVICE-OR-DOMAIN-NAME> - Optional. Clears AP, radio, or wireless client counters on a specified AP, wireless controller, service platform, or RF Domain. • <DEVICE-OR-DOMAIN-NAME> - Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
clear crypto ike sa [<IP>|all] {on <DEVICE-NAME>}
```

crypto	Clears encryption module's cached statistics
ike sa [<IP> all]	Clears IKE (Internet Key Exchange) SAs (security associations) <ul style="list-style-type: none"> • <IP> - Clears IKE SA entries for the peer identified by the <IP> keyword • all - Clears IKE SA entries for all peers
on <DEVICE-NAME>	Optional. Clears IKE SA entries, for a specified peer or all peers, on a specified device <ul style="list-style-type: none"> • <DEVICE-NAME> - Specify the name of the AP, wireless controller, or service platform.

```
clear crypto ipsec sa {on <DEVICE-NAME>}
```

crypto	Clears encryption module's cached statistics
ipsec sa {on <DEVICE-NAME>}	Clears IPsec(Internet Protocol Security) database SAs <ul style="list-style-type: none"> • on <DEVICE-NAME> - Optional. Clears IPsec SA entries on a specified device • <DEVICE-NAME> - Specify the name of the AP, wireless controller, or service platform.

```
clear eguest registration statistics
```

eguest registration statistics	Clears EGuest registration server counters. When cleared EGuest registration details are deleted, and the show > eguest > registration > statistics command output is null. This command is applicable only on the NX 95XX, NX 96XX, and VX 9000 model service platforms.
--------------------------------	---

```
clear gre stats {on <DEVICE-NAME>}
```

gre stats	Clears GRE tunnel statistics
on <DEVICE-NAME>	Optional. Clears GRE tunnel statistics on a specified device <ul style="list-style-type: none"> • <DEVICE-NAME> - Specify the name of the AP, wireless controller, or service platform.

```
clear event-history
```

event-history	Clears event history cache entries
---------------	------------------------------------

```
clear ip bgp [<IP>|all|external] {in prefix-filter} {on <DEVICE-NAME>}
```

ip bgp [<IP> all external]	<p>Clears on-going BGP sessions based on the option selected</p> <ul style="list-style-type: none"> • <IP> – Clears BGP session with the peer identified by the <IP> keyword. Specify the BGP peer's IP address. • all – Clears all BGP peer sessions • external – Clears eBGP (external BGP) peer sessions <p>This command is applicable only to the RFS 4000, NX 95XX, NX 96XX, and VX 9000 platforms.</p> <p>Modifications made to BGP settings (BGP access lists, weight, distance, route-maps, versions, routing policy, etc.) take effect only after on-going BGP sessions are cleared. The clear > ip > bgp command clears BGP sessions. To reduce lose of route updates during the process, use the 'soft' option. Soft reconfiguration stores inbound/outbound route updates to be processed later and updated to the routing table. This requires high memory usage.</p>
in prefix-filter	<p>Optional. Clears inbound route updates</p> <ul style="list-style-type: none"> • prefix-filter – Optional. Clears the existing ORF (Outbound Route Filtering) prefix-list
on <DEVICE-NAME>	<p>Optional. Clears route updates on a specified device</p> <ul style="list-style-type: none"> • <DEVICE-NAME> – Specify the name of the AP or service platform.

```
clear ip bgp [<IP>|all|external] {out} {(on <DEVICE-NAME>)}
```

ip bgp [<IP> all external]	<p>Clears on-going BGP sessions based on the option selected</p> <ul style="list-style-type: none"> • <IP> – Clears BGP session with the peer identified by the <IP> keyword. Specify the BGP peer's IP address. • all – Clears all BGP peer sessions • external – Clears eBGP peer sessions <p>This command is applicable only to the RFS 4000, NX 95XX, NX 96XX, and VX 9000 platforms.</p>
out	<p>Optional. Clears outbound route updates. Optionally specify the device on which to execute this command.</p>
on <DEVICE-NAME>	<p>The following keyword is recursive and optional.</p> <ul style="list-style-type: none"> • on <DEVICE-NAME> – Optional. Clears BGP sessions on a specified device <ul style="list-style-type: none"> • <DEVICE-NAME> – Specify the name of the AP or service platform.

```
clear ip bgp [<IP>|all|external] {soft {in/out}} {on <DEVICE-NAME>}
```


ip bgp [<IP> all external]	<p>Clears on-going BGP sessions based on the option selected</p> <ul style="list-style-type: none"> • <IP> – Clears BGP session with the peer identified by the <IP> keyword. Specify the BGP peer’s IP address. • all – Clears all BGP peer sessions • external – Clears external BGP (eBGP) peer sessions <p>This command is applicable only to the RFS 4000, NX 95XX, NX 96XX, and VX 9000 platforms.</p>
soft {in out}	<p>Optional. Initiates soft-reconfiguration of route updates for the specified IP address</p> <ul style="list-style-type: none"> • in – Optional. Enables soft reconfiguration of inbound route updates • out – Optional. Enables soft reconfiguration of outbound route updates <p>Modifications made to BGP settings (BGP access lists, weight, distance, route-maps, versions, routing policy, etc.) take effect only after on-going BGP sessions are cleared. The clear > ip > bgp command clears BGP sessions. To reduce loss of route updates during the process, use the ‘soft’ option. Soft reconfiguration stores inbound/outbound route updates to be processed later and updated to the routing table. This requires high memory usage.</p>
on <DEVICE-NAME>	<p>Optional. Initiates soft reconfiguration inbound/outbound route updates on a specified device</p> <ul style="list-style-type: none"> • <DEVICE-NAME> – Specify the name of the AP or service platform.

```
clear ip bgp process {on <DEVICE-NAME>}
```

ip bgp process	<p>Clears all BGP processes running</p> <p>This command is applicable only to the RFS 4000, NX 95XX, NX 96XX, and VX 9000 platforms.</p>
on <DEVICE-NAME>	<p>Optional. Clears all BGP processes on a specified device</p> <ul style="list-style-type: none"> • <DEVICE-NAME> – Specify the name of the AP or service platform.

```
clear ip dhcp bindings [<IP>|all] {on <DEVICE-NAME>}
```

ip	Clears a DHCP (Dynamic Host Configuration Protocol) server’s IP address binding entries
dhcp bindings	Clears DHCP connections and server bindings
<IP>	Clears specific address binding entries. Specify the IP address to clear binding entries.
all	Clears all address binding entries
on <DEVICE-NAME>	<p>Optional. Clears a specified address binding or all address bindings on a specified device</p> <ul style="list-style-type: none"> • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
clear ip ospf process {on <DEVICE-NAME>}
```

ip ospf process	Clears already enabled <i>Open Shortest Path First</i> (OSPF) process and restarts the process
on <DEVICE-NAME>	Optional. Clears OSPF process on a specified device OSPF is a link-state IGP (interior gateway protocol). OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighboring routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer, which makes routing decisions based solely on the destination IP address found in IP packets. <ul style="list-style-type: none"> • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
clear ipv6 neighbor-cache {on <DEVICE-NAME>}
```

clear ipv6 neighbor-cache	Clears IPv6 neighbor cache entries
on <DEVICE-NAME>	Optional. Clears IPv6 neighbor cache entries on a specified device <ul style="list-style-type: none"> • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
clear lacp [<1-4> counters|counters]
```

clear lacp [<1-4> counters counters]	Clears LACP (Link Aggregation Control Protocol) counters for a specified port-channel group or all port-channel groups configured <ul style="list-style-type: none"> • <1-4> counters – Clears LACP counters for a specified port-channel. Specify the port-channel index number from 1 - 4. Note, LACP is supported only on the NX 5500, NX 75XX, and NX 95XX model service platforms. However, the NX 95XX series service platforms support only two (2) port-channels, and the other model service platforms support four (4) port-channels. • counters – Clears LACP counters for all configured port-channels on the device
--------------------------------------	--

```
clear mac-address-table{address <MAC>/vlan <1-4094>} {on <DEVICE-NAME>}
```

mac-address-table	Clears MAC address forwarding table data based on the parameters passed Use this command to clear the following: all or specified MAC addresses from the system, all MAC addresses on a specified interface, all MAC addresses on a specified VLAN, or the authentication state of a MAC address.
address <MAC>	Optional. Clears a specified MAC address from the MAC address table. <ul style="list-style-type: none"> • <MAC> – Specify the MAC address in one of the following formats: AA-BB-CC-DD-EE-FF or AA:BB:CC:DD:EE:FF or AABB.CCDD.EEFF <p>Note: If executed without specifying any MAC address(es), all MAC addresses from the MAC address table will be removed.</p>

vlan <1-4094>	Optional. Clears all MAC addresses for a specified VLAN <ul style="list-style-type: none"> • <1-4094> – Specify the VLAN ID from 1 - 4094
on <DEVICE-NAME>	Optional. Clears a single MAC entry or all MAC entries, for the specified VLAN on a specified device <ul style="list-style-type: none"> • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
clear mac-address-table {interface [<IF-NAME>/ge <1-X>/port-channel <1-X>]} {on <DEVICE-NAME>}
```

mac-address-table	Clears MAC address forwarding table data based on the parameters passed Use this command to clear the following: all or specified MAC addresses from the system, all MAC addresses on a specified interface, all MAC addresses on a specified VLAN, or the authentication state of a MAC address.
interface	Clears all MAC addresses for the selected interface. Use the options available to specify the interface.
<IF-NAME>	Clears MAC address forwarding table for the specified layer 2 interface (Ethernet port) <ul style="list-style-type: none"> • <IF-NAME> – Specify the layer 2 interface name.
ge <1-X>	Clears MAC address forwarding table for the specified GigabitEthernet interface <ul style="list-style-type: none"> • <1-X> – Specify the GigabitEthernet interface index from 1 - X. <p>Note: The number of GE interfaces supported varies for different device types.</p>
port-channel <1-X>	Clears MAC address forwarding table for the specified port-channel interface <ul style="list-style-type: none"> • <1-X> – Specify the port-channel interface index from 1 - X. <p>Note: The number of port-channel interfaces supported varies for different device types.</p>
on <DEVICE-NAME>	Optional. Clears the MAC address forwarding table, for the selected interface, on a specified device <ul style="list-style-type: none"> • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
clear mac-address-table mac-auth-state address <MAC> vlan <1-4904> {on <DEVICE-NAME>}
```

mac-address-table mac-auth-state address <MAC> vlan <1-4904>	<p>Clears MAC addresses learned from a particular VLAN when WLAN MAC authentication and captive-portal fall back is enabled. Access points/controllers provide WLAN access to clients whose MAC address has been learned and stored in their MAC address tables. Use this command to clear a specified MAC address on the MAC address table. Once cleared the client has to re-authenticate, and is provided access only on successful authentication.</p> <ul style="list-style-type: none"> • <MAC> - Specify the MAC address to clear. <ul style="list-style-type: none"> • vlan <1-4904> - Specify the VLAN interface from 1 - 4094. In the AP/controller's MAC address table, the specified MAC address is cleared on the specified VLAN interface.
on <DEVICE-NAME>	<p>Optional. Clears the specified MAC address on a specified device</p> <ul style="list-style-type: none"> • <DEVICE-NAME> - Specify the name of the AP, wireless controller, or service platform. <p>Note: If a device is not specified, the system clears the MAC address on all devices.</p>

```
clear mint mlcp history {on <DEVICE-NAME>}
```

mint	Clears MINT related information
mlcp history	Clears <i>MiNT Link Creation Protocol</i> (MLCP) client history
on <DEVICE-NAME>	<p>Optional. Clears MLCP client history on a specified device</p> <ul style="list-style-type: none"> • <DEVICE-NAME> - Specify the name of the AP, wireless controller, or service platform.

```
clear role ldap-stats {on <DEVICE-NAME>}
```

role ldap-stats	Clears LDAP (Lightweight Directory Access Protocol) server statistics
on <DEVICE-NAME>	<p>Optional. Clears LDAP server statistics on a specified device</p> <ul style="list-style-type: none"> • <DEVICE-NAME> - Specify the name of the AP, wireless controller, or service platform.

```
clear rtls [aer scout|ekahau] {<MAC/DEVICE-NAME> {on <DEVICE-OR-DOMAIN-NAME>}|
on <DEVICE-OR-DOMAIN-NAME>}
```

rtls	Clears RTLS (Real Time Location Service) statistics
aer scout	Clears RTLS Aer scout statistics
ekahau	Clears RTLS Ekahau statistics

<MAC/DEVICE-NAME>	<p>This keyword is common to the 'aeroscout' and 'ekahau' parameters.</p> <ul style="list-style-type: none"> • <MAC/DEVICE-NAME> – Optional. Clears Aeroscout or Ekahau RTLS statistics on a specified AP, wireless controller, or service platform. Specify the AP's MAC address or hostname.
on <DEVICE-OR-DOMAIN-NAME>	<p>This keyword is common to the 'aeroscout' and 'ekahau' parameters.</p> <ul style="list-style-type: none"> • on <DEVICE-OR-DOMAIN-NAME> – Optional. Clears Aeroscout or Ekahau RTLS statistics on a specified AP, wireless controller, service platform, or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
clear spanning-tree detected-protocols {on <DEVICE-NAME>}
```

spanning-tree	Clears spanning tree entries on an interface and restarts protocol migration
detected-protocols	Restarts protocol migration
on <DEVICE-NAME>	<p>Optional. Clears spanning tree entries on a specified device</p> <ul style="list-style-type: none"> • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
clear spanning-tree detected-protocols {interface [<INTERFACE-NAME>|ge <1-X>|me1|port-channel <1-X>|pppoe1|up1|vlan <1-4094>|wwan1]} {on <DEVICE-NAME>}
```

spanning-tree	Clears spanning tree entries on an interface and restarts protocol migration
detected-protocols	Restarts protocol migration
interface [<INTERFACE-NAME> ge <1-X> me1 port-channel <1-X> pppoe1 up1 vlan <1-4094> wwan1]	<p>Optional. Clears spanning tree entries on different interfaces</p> <ul style="list-style-type: none"> • <INTERFACE-NAME> – Clears detected spanning tree entries on a specified interface. Specify the interface name. • ge <1-X> – Clears detected spanning tree entries for the selected GigabitEthernet interface. Select the GigabitEthernet interface index from 1 - X. • me1 – Clears FastEthernet interface spanning tree entries • port-channel <1-X> – Clears detected spanning tree entries for the selected port channel interface. Select the port channel index from 1 - X. The number of port-channel interfaces supported varies for different device types. • pppoe1 – Clears detected spanning tree entries for PPPoE (Point-to-Point Protocol over Ethernet) interface • up1 – Clears detected spanning tree entries for the WAN Ethernet interface • vlan <1-4094> – Clears detected spanning tree entries for the selected VLAN interface. Select a SVI (Switch Virtual Interface) VLAN ID from 1- 4094. • wwan1 – Clears detected spanning tree entries for wireless WAN interface.
on <DEVICE-NAME>	<p>Optional. Clears spanning tree entries on a specified device</p> <ul style="list-style-type: none"> • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
clear traffic-shape statistics class <1-4> {(on <DEVICE-NAME>)}
```

traffic-shape statistics	Clears traffic shaping statistics
class <1-4>	Clears traffic shaping statistics for a specific traffic class <ul style="list-style-type: none"> • <1-4> - Specify the traffic class from 1 - 4. <p>Note: If the traffic class is not specified, the system clears all traffic shaping statistics.</p>
on <DEVICE-NAME>	Optional. Clears traffic shaping statistics for the specified traffic class on a specified device <ul style="list-style-type: none"> • <DEVICE-NAME> - Specify the name of the access point, wireless controller, or service platform. <p>Note: For more information on configuring traffic-shape, see traffic-shape on page 1224.</p>

```
clear vrrp [error-stats|stats] {on <DEVICE-NAME>}
```

vrrp	Clears VRRP (<i>Virtual Router Redundancy Protocol</i>) statistics VRRP allows a pool of routers to be advertised as a single virtual router. This virtual router is configured by hosts as their default gateway. VRRP elects a master router, from this pool, and assigns it a virtual IP address. The master router routes and forwards packets to hosts on the same subnet. When the master router fails, one of the backup routers is elected as the master and its IP address is mapped to the virtual IP address.
error-stats	Clears global error statistics
stats	Clears VRRP related statistics
on <DEVICE-NAME>	This following keywords are common to the 'error-stats' and 'stats' parameters: <ul style="list-style-type: none"> • on <DEVICE-NAME> - Optional. Clears VRRP statistics on a specified device • <DEVICE-NAME> - Specify the name of the AP, wireless controller, or service platform.

Examples (User Exec Mode)

```
rfs4000-229D58>clear event-history
rfs4000-229D58>clear spanning-tree detected-protocols interface port-channel 1
rfs4000-229D58>clear spanning-tree detected-protocols interface ge 1
NOC-NX9500>show lldp neighbors
-----
Chassis ID: 00-18-71-D0-0B-00
System Name: ProCurve Switch 5406z1
Platform: ProCurve J8697A Switch 5406z1, revision K.12.1X, ROM K.11.03 (/sw/code/build/btm(sw_espl))
Capabilities: Bridge Router
Enabled Capabilities: Bridge Router
Local Interface: ge1, Port ID(Port Description) (outgoing port): 26(B2)
TTL: 95 sec
Management Addresses: 10.234.160.1
-----
Chassis ID: 5C-0E-8B-1C-53-2C
System Name: HM-ROUTER
Platform: RFS-4011-11110-WR, Version 5.9.1.0-016D
Capabilities: Bridge WLAN Access Point Router
Enabled Capabilities: Bridge WLAN Access Point Router
Local Interface: ge2, Port ID(Port Description) (outgoing port): ge1(ge1)
TTL: 165 sec
```

Management Addresses: 192.168.0.1,172.168.16.1,192.168.13.1,20.168.10.1

NOC-NX9500>

NOC-NX9500>clear lldp neighbors

NOC-NX9500>show lldp neighbors

NOC-NX9500>

NOC-NX9500>show cdp neighbors

Device ID	Platform	Local Interface	Port ID	Duplex
HM-ROUTER	RFS-4011-11110-WR	ge2	ge1	full

NOC-NX9500>

NOC-NX9500>clear cdp neighbors

NOC-NX9500>show cdp neighbors

Device ID	Platform	Local Interface	Port ID	Duplex
-----------	----------	-----------------	---------	--------

NOC-NX9500>

rfs4000-229D58>clear role ldap-stats

rfs4000-229D58>show role ldap-stats

No ROLE LDAP statistics found.

rfs4000-229D58>

rfs4000-229D58>show mac-address-table

BRIDGE	VLAN	PORT	MAC	STATE
1	1	ge5	00-02-B3-28-D1-55	forward
1	1	ge5	00-0F-8F-19-BA-4C	forward
1	1	ge5	B4-C7-99-5C-FA-8E	forward
1	1	ge5	00-23-68-0F-43-D8	forward
1	1	ge5	00-15-70-38-06-49	forward
1	1	ge5	00-23-68-13-9B-34	forward
1	1	ge5	B4-C7-99-58-72-58	forward
1	1	ge5	00-15-70-81-74-2D	forward

Total number of MACs displayed: 8

rfs4000-229D58>

rfs4000-229D58>clear mac-address-table address 00-02-B3-28-D1-55

rfs4000-229D58>show mac-address-table

BRIDGE	VLAN	PORT	MAC	STATE
1	1	ge5	00-0F-8F-19-BA-4C	forward
1	1	ge5	B4-C7-99-5C-FA-8E	forward
1	1	ge5	00-23-68-0F-43-D8	forward
1	1	ge5	00-15-70-38-06-49	forward
1	1	ge5	00-23-68-13-9B-34	forward
1	1	ge5	B4-C7-99-58-72-58	forward
1	1	ge5	00-15-70-81-74-2D	forward

Total number of MACs displayed: 7

rfs4000-229D58>

Examples (Priv-Exec-Mode)

NOC-NX9500#show event-history

EVENT HISTORY REPORT

Generated on '2017-12-21 10:30:56 IST' by 'admin'

2017-12-21 10:30:48	NOC-NX9500	SYSTEM	LOGIN	Successfully logged in
user 'admin' with privilege 'superuser' from 'ssh'				
2017-12-21 10:28:57	NOC-NX9500	DIAG	PWRSPPLY_FAIL	Power supply
redundancy failure				

```

2017-12-21 10:18:55      NOC-NX9500  DIAG      PWRSPPLY_FAIL      Power supply
redundancy failure
2017-12-21 10:08:52      NOC-NX9500  DIAG      PWRSPPLY_FAIL      Power supply
redundancy failure
2017-12-21 09:58:49      NOC-NX9500  DIAG      PWRSPPLY_FAIL      Power supply
redundancy failure
2017-12-21 09:48:46      NOC-NX9500  DIAG      PWRSPPLY_FAIL      Power supply
redundancy failure

```

```

--More--
NOC-NX9500#
NOC-NX9500#clear event-history
NOC-NX9500#show event-history
EVENT HISTORY REPORT
Generated on '2017-12-21 10:32:25 IST' by 'admin'

```

```

NOC-NX9500#
NOC-NX9500#show mac-address-table

```

BRIDGE	VLAN	PORT	MAC	STATE
1	1	ge1	00-18-71-D0-1B-E6	forward
1	1	ge1	74-67-F7-07-02-35	forward
1	1	ge1	84-24-8D-84-A2-24	forward
1	1	ge1	00-04-96-9C-F1-25	forward
1	1	ge1	84-24-8D-DF-9A-4C	forward
1	1	ge1	B4-C7-99-71-17-28	forward

```

Total number of MACs displayed: 6
NOC-NX9500#
NOC-NX9500#clear mac-address-table address B4-C7-99-71-17-28
NOC-NX9500#commit
NOC-NX9500#write memory
NOC-NX9500#show mac-address-table

```

BRIDGE	VLAN	PORT	MAC	STATE
1	1	ge1	00-18-71-D0-1B-E6	forward
1	1	ge1	74-67-F7-07-02-35	forward
1	1	ge1	84-24-8D-84-A2-24	forward
1	1	ge1	00-04-96-9C-F1-25	forward
1	1	ge1	84-24-8D-DF-9A-4C	forward

```

Total number of MACs displayed: 5
NOC-NX9500#

```

clock (user and privi exec modes)

Sets a device's system clock. By default all WiNG devices are shipped with the time zone and time format set to UTC and 24-hour clock respectively. If a device's clock is set without resetting the time zone, the time is displayed relative to the UTC (Universal Time Coordinated) - Greenwich Time. To display time in the local time zone format, in the device's configuration mode, use the `timezone` command. You can also reset the time zone at the RF Domain level. When configured as RF Domain setting, it applies to all devices within the domain. Configuring the local time zone prior to setting the clock is recommended. For more information on configuring RF Domain time zone, see [timezone](#).



Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
clock set <HH:MM:SS> <1-31> <MONTH> <1993-2035> {on <DEVICE-NAME>}
```

Parameters

```
clock set <HH:MM:SS> <1-31> <MONTH> <1993-2035> {on <DEVICE-NAME>}
```

clock set	Sets a device's software system clock
<HH:MM:SS>	Sets the current time (in military format hours, minutes, and seconds) Note: By default, the WiNG software displays time in the 24-hour clock format. This setting cannot be changed.
<1-31>	Sets the numerical day of the month
<MONTH>	Sets the month of the year (Jan to Dec)
<1993-2035>	Sets a valid four digit year from 1993 - 2035
on <DEVICE-NAME>	Optional. Sets the clock on a specified device <ul style="list-style-type: none">• <DEVICE-NAME> - Specify the name of the AP, wireless controller, or service platform.

Examples (User Exec Mode)

The following commands set the time zone and clock for the logged device:

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#timezone America/Los_Angeles
nx9500-6C8809>clock set 11:24:30 21 Jan 2017
nx9500-6C8809>show clock
2017-01-21 12:14:14 PST
nx9500-6C8809>
```

Note, if the clock is set without resetting the time zone, the time displays as UTC time, as shown in the following example:

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#no timezone
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#commit
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show clock
2017-01-21 19:15:55 UTC

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```

Examples (Privi Exec Mode)

```
ap8432-070235(config-device-74-67-F7-07-02-35)#timezone America/Los_Angeles
ap8432-070235#clock set 12:51:10 21 Dec 2017
ap8432-070235#show clock
2017-12-21 04:52:06 PST
ap8432-070235#
```

cluster (user and privi exec modes)

Initiates cluster context. The cluster context provides centralized management to configure all cluster members from any one member. Commands executed under this context are executed on all members of the cluster.



Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
cluster start-election
```

Parameters

```
cluster start-election
```

start-election	Starts a new cluster master election
----------------	--------------------------------------

Examples (User Exec Mode)

```
nx9500-6C8809>cluster start-election
nx9500-6C8809>
```

Examples (Privi Exec Mode)

```
rfs4000-229D58#cluster start-election
rfs4000-229D58#
```

Related Commands

create-cluster (user and privi exec modes) on page 47	Creates a new cluster on the specified device
join-cluster (user and privi exec modes) on page 77	Adds a wireless controller or service platform, as a member, to an existing cluster of controllers

connect (user and privi exec modes)

Begins a console connection to a remote device using the remote device's MiNT ID or name



Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
connect [mint-id <MINT-ID>|<REMOTE-DEVICE-NAME>]
```

Parameters

```
connect [mint-id <MINT-ID>|<REMOTE-DEVICE-NAME>]
```

mint-id <MINT-ID>	Connects to the remote system using its MiNT ID <ul style="list-style-type: none"><MINT-ID> - Specify the remote device's MiNT ID.
<REMOTE-DEVICE-NAME>	Connects to the remote system using its name <ul style="list-style-type: none"><REMOTE-DEVICE-NAME> - Specify the remote device's name.

Examples (User Exec Mode)

```
NOC-NX9500>show mint lsp-db
5 LSPs in LSP-db of 19.6C.88.09:
LSP 19.6C.88.09 at level 1, hostname "NOC-NX9500", 2 adjacencies, seqnum 1518782
LSP 19.6D.B5.D4 at level 1, hostname "RFS6K-SITE2-VLAN192", 2 adjacencies, seqnum 1971569
LSP 19.74.B4.5C at level 1, hostname "ap8132-74B45C", 1 adjacencies, seqnum 1741167
LSP 4D.83.30.A4 at level 1, hostname "ap7522-8330A4", 1 adjacencies, seqnum 518868
LSP 70.38.06.49 at level 1, hostname "RFS6K-SITE1-VLAN20", 2 adjacencies, seqnum 1389974
NOC-NX9500>
NOC-NX9500>connect mint-id 19.74.B4.5C
```

```
Entering character mode
Escape character is '^]'.

```

```
AP8432 release 5.9.2.0-029R
ap8432-74B45C login:
```

Examples (Privi Exec Mode)

```
nx9500-6C8809#connect mint-id ?
MINT-ID MiNT ID of device to connect to
```

```
nx9500-6C8809#connect mint-id 19.22.9D.58
```

```
Entering character mode
Escape character is '^]'.

```

```
RFS4000 release 5.9.2.0-012D
rfs4000-229D58 login: admin
Password:
rfs4000-229D58>
```

create-cluster (user and privi exec modes)

Creates a new device cluster, with the specified name, and assigns it an IP address and routing level

A cluster (or redundancy group) is a set of controllers or service platforms (nodes) uniquely defined by a profile configuration. Within the cluster, members discover and establish connections to other members and provide wireless network self-healing support in the event of member's failure.

A cluster's load balance is typically distributed evenly amongst its members. An administrator needs to define how often the profile is load balanced for radio distribution, as radios can come and go and members join and exit the cluster.



Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
create-cluster name <CLUSTER-NAME> ip <IP> {level [1|2]}
```

Parameters

```
create-cluster name <CLUSTER-NAME> ip <IP> {level [1|2]}
```

create-cluster	Creates a cluster
name <CLUSTER-NAME>	Configures the cluster name <ul style="list-style-type: none">• <CLUSTER-NAME> - Specify a cluster name. Define a name for the cluster that uniquely identifies its configuration or profile support requirements. The name cannot exceed 64 characters.
ip <IP>	Specifies the device's IP address used for cluster creation <ul style="list-style-type: none">• <IP> - Specify the device's IP address in the A.B.C.D format.
level [1 2]	Optional. Configures the routing level for this cluster <ul style="list-style-type: none">• 1 - Configures level 1 (local) routing• 2 - Configures level 2 (inter-site) routing

Examples (User Exec Mode)

```
rfs4000-6DB5D4>create-cluster name TechPubs ip 192.168.13.23 level 1
... creating cluster
... committing the changes
... saving the changes
Please Wait .
[OK]
rfs4000-6DB5D4>
rfs4000-6DB5D4>show context session-config include-factory | include cluster name TechPubs
  cluster name TechPubs
rfs4000-6DB5D4>
```

Examples (Priv Exec Mode)

```
rfs4000-229D58#create-cluster name TechPubs1 ip 192.168.13.8 level 2
... creating cluster
... committing the changes
... saving the changes
Please Wait .
[OK]
rfs4000-229D58#
rfs4000-229D58#show cluster configuration
```

Cluster Configuration Information

Name : TechPubs1
Configured Mode : Active
Master Priority : 128
Force configured state : Disabled
Force configured state delay : 5 minutes
Handle STP : Disabled
Radius Counter DB Sync Time : 5 minutes
rfs4000-229D58#

Related Commands

cluster (user and privi exec modes) on page 46	Initiates cluster context. The cluster context provides centralized management to configure all cluster members from any one member.
join-cluster (user and privi exec modes) on page 77	Adds a wireless controller or service platform, as a member, to an existing cluster of controllers

crypto (user and privi exec modes)

Enables digital certificate configuration and RSA Keypair management. Digital certificates are issued by CAs and contain user or device specific information, such as name, public key, IP address, serial number, company name etc. Use this command to generate, delete, export, or import encrypted RSA Keypairs and generate *Certificate Signing Request (CSR)*.

This command also enables trustpoint configuration. Trustpoints contain the CA's identity and configuration parameters.



Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
crypto [key|pki]
crypto key [export|generate|import|zeroize]
crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL> {background/on/passphrase}
crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL>
{background/passphrase <KEY-PASSPHRASE> background} {(on <DEVICE-NAME>)}
crypto key generate rsa <RSA-KEYPAIR-NAME> [2048|4096] {on <DEVICE-NAME>}
crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL> {background/on/passphrase}
crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL>
{background/passphrase <KEY-PASSPHRASE> background} {(on <DEVICE-NAME>)}
crypto key zeroize rsa <RSA-KEYPAIR-NAME> {force} {(on <DEVICE-NAME>)}
crypto pki [authenticate|export|generate|import|zeroize]
crypto pki authenticate <TRUSTPOINT-NAME> <LOCATION-URL> {background} {(on <DEVICE-NAME>)}
crypto pki export [request|trustpoint]
crypto pki export request [generate-rsa-key|short|use-rsa-key] <RSA-KEYPAIR-NAME>
[autogen-subject-name|subject-name]
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME>
autogen-subject-name [<EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>]
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME>
autogen-subject-name (<EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>)
crypto pki export request [generate-rsa-key|short [generate-rsa-key|use-rsa-key]|use-rsa-
key]
<RSA-KEYPAIR-NAME> subject-name <COMMON-NAME> <COUNTRY> <STATE> <CITY> <ORGANIZATION>
<ORGANIZATION-UNIT> (<EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>)
crypto pki export trustpoint <TRUSTPOINT-NAME> <EXPORT-TO-URL> {background/passphrase <KEY-
PASSPHRASE> background}
{(on <DEVICE-NAME>)}
crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key]
<RSA-KEYPAIR-NAME> [autogen-subject-name|subject-name]
crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key]
<RSA-KEYPAIR-NAME> autogen-subject-name {(email <SEND-TO-EMAIL>, fqdn <FQDN>,ip-address
<IP>,
on <DEVICE-NAME>)}
crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key]
<RSA-KEYPAIR-NAME> subject-name <COMMON-NAME> <COUNTRY> <STATE> <CITY> <ORGANIZATION>
<ORGANIZATION-UNIT> {(email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>,on <DEVICE-NAME>)}
crypto pki import [certificate|crl|trustpoint]
crypto pki import [certificate|crl] <TRUSTPOINT-NAME> <IMPORT-FROM-URL> {background} {(on
<DEVICE-NAME>)}
crypto pki import trustpoint <TRUSTPOINT-NAME> <IMPORT-FROM-URL> {background/passphrase
<KEY-PASSPHRASE> background} {(on <DEVICE-NAME>)}
crypto pki zeroize trustpoint <TRUSTPOINT-NAME> {del-key} {(on <DEVICE-NAME>)}
```

Parameters

```
crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL> {background/passphrase <KEY-
PASSPHRASE> background} {(on <DEVICE-NAME>)}
```

key	Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.
export rsa <RSA-KEYPAIR-NAME>	Exports an existing RSA Keypair to a specified destination <ul style="list-style-type: none"> <RSA-KEYPAIR-NAME> - Specify the RSA Keypair name.
<EXPORT-TO-URL>	Specify the RSA Keypair destination address. Both IPv4 and IPv6 address formats are supported. After specifying the destination address (where the RSA Keypair is exported), configure one of the following parameters: background or passphrase.
background	Optional. Performs export operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the export on.

passphrase <KEY-PASSPHRASE> background	Optional. Encrypts RSA Keypair before exporting <ul style="list-style-type: none"> • <KEY-PASSPHRASE> – Specify a passphrase to encrypt the RSA Keypair. • background – Optional. Performs export operation in the background. After specifying the passphrase, optionally specify the device (access point or controller) to perform the export on.
on <DEVICE-NAME>	The following parameter is recursive and common to all of the above parameters: <ul style="list-style-type: none"> • on <DEVICE-NAME> – Optional. Performs export operation on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
crypto key generate rsa <RSA-KEYPAIR-NAME> [2048|4096] {on <DEVICE-NAME>}
```

key	Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.
generate rsa <RSA-KEYPAIR-NAME> [2048 4096]	Generates a new RSA Keypair <ul style="list-style-type: none"> • <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name. • [2048 4096] – Sets the size of the RSA key in bits. The options are 2048 bits and 4096 bits. The default size is 2048 bits. <p>After specifying the key size, optionally specify the device (access point or controller) to generate the key on.</p>
on <DEVICE-NAME>	Optional. Generates the new RSA Keypair on a specified device <ul style="list-style-type: none"> • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL>
{background|passphrase <KEY-PASSPHRASE> background} {(on <DEVICE-NAME>)}
```

key	Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.
import rsa <RSA-KEYPAIR-NAME>	Imports a RSA Keypair from a specified source <ul style="list-style-type: none"> • <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name.
<IMPORT-FROM-URL>	Specify the RSA Keypair source address. Both IPv4 and IPv6 address formats are supported. After specifying the source address (where the RSA Keypair is imported from), configure one of the following parameters: background or passphrase.
background	Optional. Performs import operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the import on.

passphrase <KEY-PASSPHRASE> background	Optional. Decrypts the RSA Keypair after importing <ul style="list-style-type: none"> • <KEY-PASSPHRASE> - Specify the passphrase to decrypt the RSA Keypair. • background - Optional. Performs import operation in the background. After specifying the passphrase, optionally specify the device (access point, controller, or service platform) to perform the import on.
on <DEVICE-NAME>	The following parameter is recursive and common to the 'background' and 'passphrase' keywords: <ul style="list-style-type: none"> • on <DEVICE-NAME> - Optional. Performs import operation on a specific device • <DEVICE-NAME> - Specify the name of the AP, wireless controller, or service platform.

```
crypto key zeroize rsa <RSA-KEYPAIR-NAME> {force} {(on <DEVICE-NAME>)}
```

key	Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.
zeroize rsa <RSA-KEYPAIR-NAME>	Deletes a specified RSA Keypair <ul style="list-style-type: none"> • <RSA-KEYPAIR-NAME> - Specify the RSA Keypair name. <p>Note: All device certificates associated with this key will also be deleted.</p>
force	Optional. Forces deletion of all certificates associated with the specified RSA Keypair. Optionally specify a device on which to force certificate deletion.
on <DEVICE-NAME>	The following parameter is recursive and optional: <ul style="list-style-type: none"> • on <DEVICE-NAME> - Optional. Deletes all certificates associated with the RSA Keypair on a specified device • <DEVICE-NAME> - Specify the name of the AP, wireless controller, or service platform.

```
crypto pki authenticate <TRUSTPOINT-NAME> <URL> {background} {(on <DEVICE-NAME>)}
```

pki	Enables Private Key Infrastructure (PKI) management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated Certificate Authority (CA) certificates.
authenticate <TRUSTPOINT-NAME>	Authenticates a trustpoint and imports the corresponding CA certificate <ul style="list-style-type: none"> • <TRUSTPOINT-NAME> - Specify the trustpoint name.
url	Specify CA's location. Both IPv4 and IPv6 address formats are supported. <p>Note: The CA certificate is imported from the specified location.</p>
background	Optional. Performs authentication in the background. If selecting this option, you can optionally specify the device (access point, controller, or service platform) to perform the export on.
on <DEVICE-NAME>	The following parameter is recursive and optional: <ul style="list-style-type: none"> • on <DEVICE-NAME> - Optional. Performs authentication on a specified device • <DEVICE-NAME> - Specify the name of the AP, wireless controller, or service platform.

```
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME>  
autogen-subject-name (<EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>)
```


pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.
export request	Exports CSR to the CA for digital identity certificate. The CSR contains applicant's details and RSA Keypair's public key.
[generate-rsa-key use-rsa-key] <RSA- KEYPAIR-NAME>	Generates a new RSA Keypair or uses an existing RSA Keypair <ul style="list-style-type: none"> • generate-rsa-key – Generates a new RSA Keypair for digital authentication • use-rsa-key – Uses an existing RSA Keypair for digital authentication • <RSA-KEYPAIR-NAME> – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name.
autogen-subject- name	Auto generates subject name from configuration parameters. The subject name identifies the certificate.
<EXPORT-TO-URL>	Specify the CA's location. Both IPv4 and IPv6 address formats are supported. Note: The CSR is exported to the specified location.
email <SEND-TO- EMAIL>	Exports CSR to a specified e-mail address <ul style="list-style-type: none"> • <SEND-TO-EMAIL> – Specify the CA's e-mail address.
fqdn <FQDN>	Exports CSR to a specified Fully Qualified Domain Name (FQDN) <ul style="list-style-type: none"> • <FQDN> – Specify the CA's FQDN.
ip-address <IP>	Exports CSR to a specified device or system <ul style="list-style-type: none"> • <IP> – Specify the CA's IP address.

```
crypto pki export request [generate-rsa-key|short [generate-rsa-key|use-rsa-key]|use-rsa-
key]
<RSA-KEYPAIR-NAME> subject-name <COMMON-NAME> <COUNTRY> <STATE> <CITY> <ORGANIZATION>
<ORGANIZATION-UNIT>
(<EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>)
```

pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.
export request	Exports CSR to the CA for a digital identity certificate. The CSR contains applicant's details and RSA Keypair's public key.
[generate-rsa-key short [generate-rsa-key use-rsa- key] use-rsa-key] <RSA- KEYPAIR-NAME>	Generates a new RSA Keypair or uses an existing RSA Keypair <ul style="list-style-type: none"> • generate-rsa-key – Generates a new RSA Keypair for digital authentication • short [generate-rsa-key use-rsa-key] – Generates and exports a shorter version of the CSR <ul style="list-style-type: none"> • generate-rsa-key – Generates a new RSA Keypair for digital authentication. If generating a new RSA Keypair, specify a name for it. • use-rsa-key – Uses an existing RSA Keypair for digital authentication. If using an existing RSA Keypair, specify its name. • use-rsa-key – Uses an existing RSA Keypair for digital authentication <ul style="list-style-type: none"> • <RSA-KEYPAIR-NAME> – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name.
subject-name <COMMON- NAME>	Configures a subject name, defined by the <COMMON-NAME> keyword, to identify the certificate <ul style="list-style-type: none"> • <COMMON-NAME> – Specify the common name used with the CA certificate. The name should enable you to identify the certificate easily (2 to 64 characters in length).

<COUNTRY>	Sets the deployment country code (2 character ISO code)
<STATE>	Sets the state name (2 to 64 characters in length)
<CITY>	Sets the city name (2 to 64 characters in length)
<ORGANIZATION>	Sets the organization name (2 to 64 characters in length)
<ORGANIZATION-UNIT>	Sets the organization unit (2 to 64 characters in length)
<EXPORT-TO-URL>	Specify the CA's location. Both IPv4 and IPv6 address formats are supported. The CSR is exported to the specified location.
email <SEND-TO-EMAIL>	Exports CSR to a specified e-mail address <ul style="list-style-type: none"> <SEND-TO-EMAIL> - Specify the CA's e-mail address.
fqdn <FQDN>	Exports CSR to a specified FQDN <ul style="list-style-type: none"> <FQDN> - Specify the CA's FQDN.
ip-address <IP>	Exports CSR to a specified device or system <ul style="list-style-type: none"> <IP> - Specify the CA's IP address.

```
crypto pki export trustpoint <TRUSTPOINT-NAME> <EXPORT-TO-URL>
{background/passphrase <KEY-PASSPHRASE> background} {(on <DEVICE-NAME>)}
```

pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.
export trustpoint <TRUSTPOINT-NAME>	Exports a trustpoint along with CA certificate, Certificate Revocation List (CRL), server certificate, and private key <ul style="list-style-type: none"> <TRUSTPOINT-NAME> - Specify the trustpoint name (should be authenticated).
<EXPORT-TO-URL>	Specify the destination address. Both IPv4 and IPv6 address formats are supported. The trustpoint is exported to the address specified here.
background	Optional. Performs export operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the export on
passphrase <KEY-PASSPHRASE> background	Optional. Encrypts the key with a passphrase before exporting <ul style="list-style-type: none"> <KEY-PASSPHRASE> - Specify the passphrase to encrypt the trustpoint. background - Optional. Performs export operation in the background. After specifying the passphrase, optionally specify the device (access point or controller) to perform the export on.
on <DEVICE-NAME>	The following parameter is recursive and common to the 'background' and 'passphrase' keywords: <ul style="list-style-type: none"> on <DEVICE-NAME> - Optional. Performs export operation on a specified device <DEVICE-NAME> - Specify the name of the AP, wireless controller, or service platform.

```
crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key]
<RSA-KEYPAIR-NAME> autogen-subject-name {(email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address
<IP>,
on <DEVICE-NAME>)}
```

pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated certificates.
generate	Generates a certificate and a trustpoint

self-signed <TRUSTPOINT-NAME>	Generates a self-signed certificate and a trustpoint <ul style="list-style-type: none"> • <TRUSTPOINT-NAME> – Specify a name for the certificate and its trustpoint.
[generate-rsa-key use-rsa-key] <RSA-KEYPAIR-NAME>	Generates a new RSA Keypair, or uses an existing RSA Keypair <ul style="list-style-type: none"> • generate-rsa-key – Generates a new RSA Keypair for digital authentication • use-rsa-key – Uses an existing RSA Keypair for digital authentication <ul style="list-style-type: none"> • <RSA-KEYPAIR-NAME> – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name.
autogen-subject-name	Auto generates the subject name from the configuration parameters. The subject name helps to identify the certificate.
email <SEND-TO-EMAIL>	Optional. Exports the self-signed certificate to a specified e-mail address <ul style="list-style-type: none"> • <SEND-TO-EMAIL> – Specify the e-mail address.
fqdn <FQDN>	Optional. Exports the self-signed certificate to a specified FQDN <ul style="list-style-type: none"> • <FQDN> – Specify the FQDN.
ip-address <IP>	Optional. Exports the self-signed certificate to a specified device or system <ul style="list-style-type: none"> • <IP> – Specify the device’s IP address.
on <DEVICE-NAME>	Optional. Exports the self-signed certificate on a specified device <ul style="list-style-type: none"> • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key]
<RSA-KEYPAIR-NAME> subject-name <COMMON-NAME> <COUNTRY> <STATE> <CITY> <ORGANIZATION>
<ORGANIZATION-UNIT> { (email <SEND-TO-EMAIL>, fqdn <FQDN>, ip-address <IP>, on <DEVICE-NAME> ) }
```

pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated certificates.
generate self-signed <TRUSTPOINT-NAME>	Generates a self-signed certificate and a trustpoint <ul style="list-style-type: none"> • <TRUSTPOINT-NAME> – Specify a name for the certificate and its trustpoint.
[generate-rsa-key use-rsa-key] <RSA-KEYPAIR-NAME>	Generates a new RSA Keypair, or uses an existing RSA Keypair <ul style="list-style-type: none"> • generate-rsa-key – Generates a new RSA Keypair for digital authentication • use-rsa-key – Uses an existing RSA Keypair for digital authentication <ul style="list-style-type: none"> • <RSA-KEYPAIR-NAME> – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name.
subject-name <COMMON-NAME>	Configures a subject name, defined by the <COMMON-NAME> keyword, to identify the certificate <ul style="list-style-type: none"> • <COMMON-NAME> – Specify the common name used with this certificate. The name should enable you to identify the certificate easily and should not exceed 2 to 64 characters in length.
<COUNTRY>	Sets the deployment country code (2 character ISO code)
<STATE>	Sets the state name (2 to 64 characters in length)
<CITY>	Sets the city name (2 to 64 characters in length)
<ORGANIZATION>	Sets the organization name (2 to 64 characters in length)
<ORGANIZATION-UNIT>	Sets the organization unit (2 to 64 characters in length)

email <SEND-TO-EMAIL>	Optional. Exports the self-signed certificate to a specified e-mail address <ul style="list-style-type: none"> • <SEND-TO-EMAIL> – Specify the e-mail address.
fqdn <FQDN>	Optional. Exports the self-signed certificate to a specified FQDN <ul style="list-style-type: none"> • <FQDN> – Specify the FQDN.
ip-address <IP>	Optional. Exports the self-signed certificate to a specified device or system <ul style="list-style-type: none"> • <IP> – Specify the device’s IP address.

```
crypto pki import [certificate|crl] <TRUSTPOINT-NAME> <IMPORT-FROM-URL>
{background} {(on <DEVICE-NAME>)}
```

pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.
import	Imports certificates, Certificate Revocation List (CRL), or a trustpoint to the selected device
[certificate crl] <TRUSTPOINT-NAME>	Imports a signed server certificate or CRL <ul style="list-style-type: none"> • certificate – Imports signed server certificate • crl – Imports CRL • <TRUSTPOINT-NAME> – Specify the trustpoint name (should be authenticated).
<IMPORT-FROM-URL>	Specify the signed server certificate or CRL source address. Both IPv4 and IPv6 address formats are supported. The server certificate or the CRL (based on the parameter passed in the preceding step) is imported from the location specified here.
background	Optional. Performs import operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the import on.
on <DEVICE-NAME>	The following parameter is recursive and optional: <ul style="list-style-type: none"> • on <DEVICE-NAME> – Optional. Performs import operation on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
crypto pki import trustpoint <TRUSTPOINT-NAME> <IMPORT-FROM-URL>
{background/passphrase <KEY-PASSPHRASE> background} {(on <DEVICE-NAME>)}
```

pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.
import	Imports certificates, CRL, or a trustpoint to the selected device
trustpoint <TRUSTPOINT-NAME>	Imports a trustpoint and its associated CA certificate, server certificate, and private key <ul style="list-style-type: none"> • <TRUSTPOINT-NAME> – Specify the trustpoint name (should be authenticated).
<IMPORT-FROM-URL>	Specify the trustpoint source address. Both IPv4 and IPv6 address formats are supported.
background	Optional. Performs import operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the import on.

passphrase <KEY-PASSPHRASE> background	Optional. Decrypts trustpoint with a passphrase after importing <ul style="list-style-type: none"> • <KEY-PASSPHRASE> – Specify the passphrase. After specifying the passphrase, optionally specify the device to perform import on. • background – Optional. Performs import operation in the background. After specifying the passphrase, optionally specify the device (access point or controller) to perform the import on.
on <DEVICE-NAME>	The following parameter is recursive and optional: <ul style="list-style-type: none"> • on <DEVICE-NAME> – Optional. Performs import operation on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
crypto pki zeroize trustpoint <TRUSTPOINT-NAME> {del-key} {(on <DEVICE-NAME>)}
```

pki	Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.
zeroize trustpoint <TRUSTPOINT-NAME>	Imports certificates, <i>Certificate Revocation List</i> (CRL), or a trustpoint to the selected device
[certificate crl] <TRUSTPOINT-NAME>	Deletes a trustpoint and its associated CA certificate, server certificate, and private key <ul style="list-style-type: none"> • <TRUSTPOINT-NAME> – Specify the trustpoint name (should be authenticated).
del-key	Optional. Deletes the private key associated with the server certificate. Optionally specify the device to perform deletion on.
on <DEVICE-NAME>	The following parameter is recursive and optional: <ul style="list-style-type: none"> • on <DEVICE-NAME> – Optional. Deletes the trustpoint on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Usage Guidelines

The system supports both IPv4 and IPv6 address formats. Provide source and destination locations using any one of the following options:

- IPv4 URLs:

```
tftp://<hostname|IPv4>[:port]/path/file
```

```
ftp://<user>:<passwd>@<hostname|IPv4>[:port]/path/file
```

```
sftp://<user>@<hostname|IPv4>[:port]/path/file
```

```
http://<hostname|IPv4>[:port]/path/file
```

```
cf:/path/file usb<n>:/path/file
```

- IPv6 URLs:

```
tftp://<hostname|IPv6>[:port]/path/file
```

```
ftp://<user>:<passwd>@<hostname|IPv6>[:port]/path/file
```

```
sftp://<user>@<hostname|IPv6>[:port]/path/file
```

```
http://<hostname|IPv6>[:port]/path/file
```

Examples (User Exec Mode)

```
rfs4000-229D58>crypto key generate rsa key 1025
RSA Keypair successfully generated
rfs4000-229D58>
rfs4000-229D58>crypto key import rsa test123 url passphrase word background
RSA key import operation is started in background
rfs4000-229D58>
rfs4000-229D58>crypto pki generate self-signed word generate-rsa-key word autogen-subject-
name fqdn word
Successfully generated self-signed certificate
rfs4000-229D58>
rfs4000-229D58>crypto pki zeroize trustpoint word del-key
Successfully removed the trustpoint and associated certificates
%Warning: Applications associated with the trustpoint will start using default-trustpoint
rfs4000-229D58>
rfs4000-229D58>crypto pki authenticate word url background
Import of CA certificate started in background
rfs4000-229D58>
rfs4000-229D58>crypto pki import trustpoint word url passphrase word
Import operation started in background
rfs4000-229D58>
```

Examples (Privi Exec Mode)

```
NOC-NX9500#crypto key generate rsa key 2048
RSA key size > 2048. Key generation started in background.
NOC-NX9500#c
```

Related Commands

<code>no (user exec mode)</code> on page 83	Removes server certificates, trustpoints and their associated certificates
---	--

crypto-cmp-cert-policy (user and privi exec modes)

Triggers a Certificate Management Protocol (CMP) certificate update on a specified device or devices



Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
crypto-cmp-cert-update <TRUSTPOINT-NAME> {on <DEVICE-NAME>}
```

Parameters

```
crypto-cmp-cert-update <TRUSTPOINT-NAME> {on <DEVICE-NAME>}
```

```
crypto-cmp-cert-update
<TRUSTPOINT-NAME> on
<DEVICE-NAME>
```

Triggers a CMP certificate update on a specified device or devices

- <TRUSTPOINT-NAME> - Specify the target trustpoint name. A trustpoint represents a CA/identity pair containing the identity of the CA, CA specific configuration parameters, and an association with an enrolled identity certificate. Use the crypto-cmp-policy context mode to configure the trustpoint.
- on <DEVICE-NAME> - Optional. Initiates a CMP certificate update and response on a specified device or devices. Specify the name of the AP, wireless controller, or service platform. Multiple devices can be provided as a comma separated list.
 - <DEVICE-NAME> - Specify the name of the AP, wireless controller, or service platform.

Example (User Exec Mode)

```
rfs4000-229D58>crypto-cmp-cert-update test on B4-C7-99-71-17-28
CMP Cert update success
rfs4000-229D58>
```

Example (Privi Exec Mode)

```
NOC-NX9500#crypto-cmp-cert-update test on NOC-NX9500
CMP Cert update success
NOC-NX9500#
```

database (user and privi exec modes)

Enables automatic repairing (vacuuming) and dropping of captive-portal and NSight databases

If enforcing authenticated access to the database, use this command to generate the keyfile. Every keyfile has a set of associated users having a username and password. Access to the database is allowed only if the user credentials entered during database login are valid. For more information on enabling database authentication, see [Enabling Database Authentication](#).



Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 96XX, VX 9000

Syntax

```
database [drop|keyfile|repair]
database drop [all|captive-portal|nsight]
database repair {on <DEVICE-NAME>}
database keyfile [export|generate|import|zerzoise]
database keyfile generate
database keyfile [export|import] <URL>
database keyfile zerzoise
```

Parameters

```
database drop [all|captive-portal|nsight]
```

database drop [all|captive-portal|nsight]

Drops (deletes) all or a specified database. Execute the command on the database.

- all – Drops all databases, captive portal and NSight
- captive-portal – Drops the captive-portal database
- nsight – Drops the NSight database

database repair {on <DEVICE-NAME>}

database repair on <DEVICE-NAME>

Enables automatic repairing of all databases. Repairing (vacuuming a database refers to the process of finding and reclaiming space left over from previous DELETE statements. Execute the command on the database host.

- on <DEVICE-NAME> – Optional. Specifies the name of the database host. When specified, databases on the specified host are periodically checked to identify and remove obsolete data documents.
- <DEVICE-NAME> – Specify the name of the access point, wireless controller, or service platform.

Note: If no device is specified, the system repairs all databases.

database keyfile generate

database keyfile generate

Enables database keyfile management. This command is part of a set of configurations required to enforce database authentication. Use this command to generate database keyfiles. After generating the keyfile, create the username and password combination required to access the database. For information on creating database users see, [service](#) on page 647. For information on enabling database authentication, see [Enabling Database Authentication](#).

- generate – Generates the keyfile. In case of a replica-set deployment, execute the command on the primary database host. Once generated, export the keyfile to a specified location from where it is imported on to the replica-set hosts.

database keyfile [export|import] <URL>

database keyfile [export|import] <URL>

Enables database keyfile management. This command is part of a set of configurations required to enforce database authentication. Use this command to exchange keyfiles between replica set members.

- export – Exports the keyfile to a specified location on an FTP/SFTP/TFTP server. Execute the command on the database host on which the keyfile has been generated.
- import – Imports the keyfile from a specified location. Execute the command on the replica set members.

The following parameter is common to both of the above keywords:

- <URL> – Specify the location to/from where the keyfile is to be exported/imported. Use one of the following options to specify the keyfile location:

ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file

sftp://<user>:<passwd>@<hostname|IP>[:port]/path/file

tftp://<hostname|IP>[:port]/path/file

database keyfile zerzoise

database keyfile zerzoise

Enables database keyfile management. Use this command to delete keyfiles

- zerzoise – Deletes an existing keyfile.

Example (User Exec Mode)

```
nx9500-6C8809nx9500-6C8809>database repair on nx9500-6C8809
nx9500-6C8809>
nx9500-6C8809>database keyfile generate
Database keyfile successfully generated
nx9500-6C8809nx9500-6C8809>
nx9500-6C8809>database keyfile zeroize
Database keyfile successfully removed
nx9500-6C8809nx9500-6C8809>
```

Example (Privl Exec Mode)

```
vx9000-1A1809#database keyfile generate
Database keyfile successfully generated
vx9000-1A1809#
vx9000-1A1809#database keyfile export ftp://1.1.1.111/db-key
Database keyfile successfully exported
vx9000-1A1809#
vx9000-D031F2#database keyfile import ftp://1.1.1.111/db-key
Database keyfile successfully imported
vx9000-D031F2#
```

Example: Enabling Database Authentication

Follow the steps below to enable database authentication.

- 1 On the primary database host,
 - a Generate the database keyfile.

```
Primary-DB-HOST>database keyfile generate
Database keyfile successfully generated
Primary-DB-HOST>
```
 - b Use the **show > database > keyfile** command to view the generated keyfile.

- c Export the keyfile to an external location. This is required only in case of database replica-set deployment.
- ```
Primary-DB-HOST>database keyfile export ftp://1.1.1.111/db-key
Database keyfile successfully exported
Primary-DB-HOST>
```
- d Create the users that are allowed access to the database.
- ```
Primary-DB-HOST#service database authentication create-user username techpubs
password techPubs@123
Database user [techpubs] created.
Primary-DB-HOST#
```
- e View the database user account created.
- ```
Primary-DB-HOST#show database users

 DATABASE USER

 techpubs

Primary-DB-HOST#
```
- 2 On the replica set host, import the keyfile from the location specified in Step 1 c.
- ```
Secondary-DB-HOST#database keyfile import ftp://1.1.1.111/db-key
```
- 3 In the database-policy context, --- (used on the NSight/EGuest database hosts)
- a Enable authentication.
- ```
Primary-DB-HOST(config-database-policy-techpubs)#authentication
```
- b Configure the user accounts created in Step 1 d.
- ```
Primary-DB-HOST(config-database-policy-techpubs)#authentication username techpubs
password S540QFZz9LzSOdX1ZJEqDgAAAy3b7Gty04Z/Ih2ruxn0Ynr
Primary-DB-HOST(config-database-policy-techpubs)#show context
database-policy techpubs
authentication
authentication username techpubs password 2 S540QFZz9LzSOdX1ZJEqDgAAAy3b7Gty04Z/
Ih2ruxn0Ynr
replica-set member nx7500-A02B91 arbiter
replica-set member vx9000-1A1809 priority 1
replica-set member vx9000-D031F2 priority 20
Primary-DB-HOST(config-database-policy-techpubs)#
```
- 4 In the database-client policy context --- (used on the NSight/EGuest server host), Note, this configuration is required only if the NSight/EGuest server and database are hosted on separate hosts.
- a Configure the user credentials created in Step 1 d.
- ```
NOC-Controller(config-database-client-policy-techpubs)#authentication username
techpubs password S540QFZz9LzSOdX1ZJEqDgAAAy3b7Gty04Z/Ih2ruxn0Ynr
```
- b View the configuration.
- ```
NOC-Controller(config-database-client-policy-techpubs)#show context
database-client-policy techpubs
authentication username techpubs password 2 S540QFZz9LzSOdX1ZJEqDgAAAy3b7Gty04Z/
Ih2ruxn0Ynr
NOC-Controller(config-database-client-policy-techpubs)#
```

Related Commands

database-backup (user and privi exec modes) on page 63	Backs up captive-portal and/or NSight database to a specified location and file on an FTP or SFTP server
database-restore (user and privi exec modes) on page 64	Restores a previously exported database [captive-portal and/or NSight]

database-policy global config on page 363	Documents database-policy configuration commands. Use this option to enable the database.
database-client-policy global-config on page 359	Documents database-client-policy configuration commands. Use this option to configure the database host details (IP address or hostname). If enforcing database authentication, use it to configure the users having database access. Once configured, use the policy in the NSight/EGuest server's device config context.
service on page 647	Documents the database user account configuration details

database-backup (user and privi exec modes)

Backs up captive-portal and/or NSight database to a specified location and file on an FTP, SFTP, or TFTP server. Execute this command on the database host.



Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 96XX, VX 9000

Syntax

```
database-backup database [captive-portal|nsight|nsight-placement-info] <URL>
database-backup database [captive-portal|nsight] <URL>
database-backup database nsight-placement-info <URL>
```

Parameters

```
database-backup database [captive-portal|nsight] <URL>
```

database-backup database [captive-portal nsight]	Backs up captive portal and/or NSight database to a specified location. Select the database to backup: <ul style="list-style-type: none"> • captive-portal - Backs up captive portal database • nsight - Backs up NSight database After specifying the database type, configure the destination location.
<URL>	Configures the destination location. The database is backed up at the specified location. Specify the location URL in one of the following formats: ftp://<user>:<passwd>@<hostname IP>[:port]/path/file.tar.gz sftp://<user>:<passwd>@<hostname IP>[:port]/path/file.tar.gz

```
database-backup database nsight-placement-info <URL>
```

database-backup database nsight-placement-info <URL>	Backs up the NSight access point placement related details to a specified location <ul style="list-style-type: none"> • <URL> - Specify the URL in one of the following formats: ftp://<user>:<passwd>@<hostname IP>[:port]/path/file.tar.gz sftp://<user>:<passwd>@<hostname IP>[:port]/path/file.tar.gz tftp://<hostname IP>[:port]/path/file.tar.gz
--	--

Example (User Exec Mode)

```
NS-DB-nx9510-6C87EF>database-backup database nsight tftp://192.168.9.50/testbckup
NS-DB-nx9510-6C87EF>show database backup-status
Last Database Backup Status : In_Progress(Starting tftp transfer.)
Last Database Backup Time   : 2018-01-01 12:48:05
NS-DB-nx9510-6C87EF>show database backup-status
Last Database Backup Status : Successful
Last Database Backup Time   : Mon Jan 01 12:48:08 IST 2018
NS-DB-nx9510-6C87EF>
```

Example (Privi Exec Mode)

```
NS-DB-nx9510-6C87EF#database-backup database nsight-placement-info tftp://192.168.9.50/
plmentinfo
NS-DB-nx9510-6C87EF#show database backup-status
Last Database Backup Status : Successful
Last Database Backup Time   : Mon Jan 01 12:48:48 IST 2018
NS-DB-nx9510-6C87EF#
```

Related Commands

database (user and privi exec modes) on page 59	Enables automatic repairing (vacuuming) and dropping of databases (captive-portal and/or NSight)
database-restore (user and privi exec modes) on page 64	Restores a previously exported (backed up) database (captive-portal and/or NSight)]

database-restore (user and privi exec modes)

Restores a previously exported database [captive-portal and/or NSight]. Previously exported databases (backed up to a specified FTP or SFTP server) are restored from the backed-up location to the original database.



Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 96XX, VX 9000

Syntax

```
database-restore database [captive-portal|nsight] <URL>
```

Parameters

```
database-restore database [captive-portal|nsight] <URL>
```

database-restore database [captive-portal nsight]	Restores previously exported (backed up) captive-portal and/or NSight database. Specify the database type: <ul style="list-style-type: none"> • captive-portal – Restores captive portal database • nsight – Restores NSight database After specifying the database type, configure the destination location and file name from where the files are restored.
<URL>	Configures the destination location. The database is restored from the specified location. Specify the location URL in one of the following formats: ftp://<user>:<passwd>@<hostname IP>[:port]/path/file.tar.gz sftp://<user>:<passwd>@<hostname IP>[:port]/path/file.tar.gz tftp://<hostname IP>[:port]/path/file.tar.gz

Example (User Exec Mode)

```
nx9500-6C8809>database-restore database nsight ftp://anonymous:anonymous@192.168.13.10/backups/nsight/nsight.tar.gz
```

Example (Privi Exec Mode)

```
nx9500-6C874D#database-restore database nsight ftp://anonymous:anonymous@192.168.13.10/backups/nsight/nsight.tar.gz
```

Related Commands

database (user and privi exec modes) on page 59	Enables automatic repairing (vacuuming) and dropping of databases (captive-portal and NSight)
database-backup (user and privi exec modes) on page 63	Backs up captive-portal and/or NSight database to a specified location and file on an FTP or SFTP server

device-upgrade (user and privi exec modes)

Enables firmware upgrade on an adopted device or a set of adopted devices (Access Points, wireless controllers, and service platforms)



Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

In an HM (hierarchically managed) network, this command enables centralized device upgradation across the network.

The WiNG HM network defines a three-tier structure, consisting of multiple wireless sites managed by a single NOC (Network Operations Center) controller. The NOC controller constitutes the first and the site controllers constitute the second tier of the hierarchy respectively. The site controllers may or may not be grouped to form clusters. The site controllers in turn adopt and manage access points that form the third tier of the hierarchy.



Note

Hierarchical management allows the NOC controller to upgrade controllers and access points that are directly or indirectly adopted to it. However, ensure that the NOC controller is loaded with the correct firmware version.

Use the device-upgrade command to schedule firmware upgrades across adopted devices within the network. Devices are upgraded based on their device names, MAC addresses, or RF Domain.



Note

If the persist-images option is selected, the RF Domain manager retains the old firmware image, or else deletes it. For more information on enabling device upgrade on profiles and devices (including the 'persist-images' option), see [device-upgrade](#) on page 981.



Note

A NOC controller's capacity is equal to, or higher than that of a site controller. The following devices can be deployed at NOC and sites:

- NOC controller – NX 95XX, NX 96XX, VX 9000
- Site controller – RFS 4000, NX 5500, or NX 75XX



Note

Standalone devices have to be manually upgraded.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000, RFS 6000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
device-upgrade [<MAC/HOSTNAME>|all|ap6522|ap6562|ap7161|ap7502|ap7522|ap7532|ap7602|
ap7612|ap7622|ap7632|ap7662|ap8163|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx9000|nx9600|
vx9000|cancel-upgrade|load-image|rf-domain]
device-upgrade <MAC/HOSTNAME> {no-reboot|reboot-time <TIME>/upgrade-time <TIME>
{no-reboot|reboot-time <TIME>}}
device-upgrade all {no-reboot|reboot-time <TIME>/upgrade-time <TIME>
{no-reboot|reboot-time <TIME>}} {(staggered-reboot)}
device-upgrade [ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|
ap7632|ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx9000|nx9600|vx9000] all
{force|no-reboot|reboot-time <TIME>/upgrade-time <TIME> {no-reboot|reboot-time <TIME>}}
{(staggered-reboot)}
device-upgrade cancel-upgrade [<MAC/HOSTNAME>|all|ap6522|ap6562|ap71xx|ap7502|ap7522|
ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|
nx75xx|nx9000|nx9600|vx9000|on rf-domain [<RF-DOMAIN-NAME>|all]]
device-upgrade load-image [ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|
ap7612|ap7622|ap7632|ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx9000|nx9600|vx9000]
{<IMAGE-URL>/on <DEVICE-OR-DOMAIN-NAME>}
device-upgrade rf-domain [<RF-DOMAIN-NAME>|all|containing <WORD>|filter location <WORD>]
[all|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap76232|
ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx9000|nx9600|vx9000]
{(<MAC/HOSTNAME>|force|from-controller|no-reboot|reboot-time <TIME>/staggered-reboot|
upgrade-time <TIME>)}
```

Parameters

```
device-upgrade <MAC/HOSTNAME> {no-reboot|reboot-time <TIME>/upgrade-time <TIME>
{no-reboot|reboot-time <TIME>}}
```

<MAC/HOSTNAME>	Upgrades firmware on the device identified by the <MAC/HOSTNAME> keyword <ul style="list-style-type: none"> • <MAC/HOSTNAME> - Specify the device's MAC address or hostname.
no-reboot	Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)
reboot-time <TIME>	Optional. Schedules an automatic reboot after a successful upgrade <ul style="list-style-type: none"> • <TIME> - Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.
upgrade-time <TIME> {no-reboot reboot-time <TIME>}	Optional. Schedules an automatic device firmware upgrade <ul style="list-style-type: none"> • <TIME> - Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format. The following actions can be performed after a scheduled upgrade: <ul style="list-style-type: none"> • no-reboot - Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted) • reboot-time <TIME> - Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.

```
device-upgrade all {force/no-reboot/reboot-time <TIME>/upgrade-time <TIME>
{no-reboot/reboot-time <TIME>}} {(staggered-reboot)}
```

all	Upgrades firmware on all devices
force	Optional. Select this option to force upgrade on the selected device(s). When selected, the devices are upgraded even if they have the same firmware as the upgrading access point, wireless controller, or service platform. If forcing a device upgrade, optionally specify any one of the following options: no-reboot, reboot-time, upgrade-time, or staggered-reboot.
no-reboot	Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)
reboot-time <TIME>	Optional. Schedules an automatic reboot after a successful upgrade <ul style="list-style-type: none"> • <TIME> - Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.
upgrade-time <TIME> {no-reboot reboot-time <TIME>}	Optional. Schedules an automatic firmware upgrade on all devices, of the specified type, on a specified day and time <ul style="list-style-type: none"> • <TIME> - Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format. The following actions can be performed after a scheduled upgrade: <ul style="list-style-type: none"> • no-reboot - Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted) • reboot-time <TIME> - Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.
staggered-reboot	This keyword is recursive and common to all of the above. <ul style="list-style-type: none"> • Optional. Enables staggered reboot (one at a time), without network impact

```
device-upgrade [ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|
ap7622|ap7632|ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx9000|nx9600|vx9000]
all {force/no-reboot/reboot-time <TIME>/upgrade-time <TIME>
{no-reboot/reboot-time <TIME>}} {(staggered-reboot)}
```

device-upgrade <DEVICE-TYPE> all	Upgrades firmware on all devices of a specific type. Select the device type. The options are: AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533, RFS 4000, NX 5500, NX 75XX, NX 95XX, NX 96XX, and VX 9000. After selecting the device type, schedule an automatic upgrade and/or an automatic reboot.
force	Optional. Select this option to force upgrade on the selected device(s). When selected, the devices are upgraded even if they have the same firmware as the upgrading access point, wireless controller, or service platform. If forcing a device upgrade, optionally specify any one of the following options: no-reboot, reboot-time, upgrade-time, or staggered-reboot.
no-reboot	Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)
reboot-time <TIME>	Optional. Schedules an automatic reboot after a successful upgrade <ul style="list-style-type: none"> • <TIME> – Optional. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.
upgrade-time <TIME> {no-reboot reboot-time <TIME>}	Optional. Schedules an automatic firmware upgrade on all devices, of the specified type, on a specified day and time <ul style="list-style-type: none"> • <TIME> – Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format. The following actions can be performed after a scheduled upgrade: <ul style="list-style-type: none"> • no-reboot – Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted) • reboot-time <TIME> – Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.
staggered-reboot	This keyword is recursive and common to all of the above. <ul style="list-style-type: none"> • Optional. Enables staggered reboot (one at a time), without network impact

```
device-upgrade cancel-upgrade [<MAC/HOSTNAME>|all|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx9000|nx9600|vx9000|on rf-domain [<RF-DOMAIN-NAME>|all]]
```

cancel-upgrade	Cancels a scheduled firmware upgrade based on the parameters passed. This command provides the following options to cancel scheduled firmware upgrades: <ul style="list-style-type: none"> • Cancels upgrade on specific device(s). The devices are identified by their MAC addresses or hostnames. • Cancels upgrade on all devices within the network • Cancels upgrade on all devices of a specific type. Specify the device type. • Cancels upgrade on specific device(s) or all device(s) within a specific RF Domain or all RF Domains. Specify the RF Domain name.
cancel-upgrade [<MAC/ HOSTNAME> all]	Cancels a scheduled firmware upgrade on a specified device or on all devices <ul style="list-style-type: none"> • <MAC/HOSTNAME> – Cancels a scheduled upgrade on the device identified by the <MAC/HOSTNAME> keyword. Specify the device's MAC address or hostname. • all – Cancels scheduled upgrade on all devices

cancel-upgrade <DEVICE-TYPE> all	Cancels scheduled firmware upgrade on all devices of a specific type. Select the device type. The options are: AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533, RFS 4000, NX 5500, NX 75XX, NX 95XX, NX 96XX, and VX 9000.
cancel-upgrade on rf-domain [<RF- DOMAIN-NAME> all]	Cancels scheduled firmware upgrade on all devices in a specified RF Domain or all RF Domains <ul style="list-style-type: none"> • <RF-DOMAIN-NAME> - Cancels scheduled device upgrade on all devices in a specified RF Domain. Specify the RF Domain name. • all - Cancels scheduled device upgrade on all devices across all RF Domains

```
device-upgrade load-image [ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|
ap7612|ap7622|ap7632|ap7662|ap81xx|ap8432|ap8533|rfs4000|nx500|nx9000|nx9600|vx9000]
{<IMAGE-URL>/on <DEVICE-OR-DOMAIN-NAME>}
```

load-image <DEVICE-TYPE>	Loads device firmware image from a specified location. Use this command to specify the device type and the location of the corresponding image file. <ul style="list-style-type: none"> • <DEVICE-TYPE> - Specify the device type. The options are: AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533, RFS 4000, NX 5500, NX 75XX, NX 95XX, NX 96XX, and VX 9000. <p>After specifying the device type, provide the location of the required device firmware image.</p>
<IMAGE-URL>	Specify the device's firmware image location in one of the following formats: IPv4 URLs: <ul style="list-style-type: none"> • tftp://<hostname IP>[:port]/path/file • ftp://<user>:<passwd>@<hostname IP>[:port]/path/file • sftp://<user>:<passwd>@<hostname IP>[:port]/path/file • http://<hostname IP>[:port]/path/file • cf:/path/file • usb<n>:/path/file IPv6 URLs: <ul style="list-style-type: none"> • tftp://<hostname IPv6>[:port]/path/file • ftp://<user>:<passwd>@<hostname IPv6>[:port]/path/file • sftp://<user>:<passwd>@<hostname IPv6>[:port]/path/file • http://<hostname IPv6>[:port]/path/file
on <DEVICE-OR-DOMAIN- NAME>	Specify the name of the device or RF Domain. The image, of the specified device type is loaded from the device specified here. In case of an RF Domain, the image available on the RF Domain manager is loaded. <ul style="list-style-type: none"> • <DEVICE-OR-DOMAIN-NAME> - Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
device-upgrade rf-domain [<RF-DOMAIN-NAME>|all|containing <WORD>|
filter location <WORD>] [all|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|
ap7612|ap7622|ap7632|ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx9000|nx9600|
vx9000] {( <MAC/HOSTNAME>/force/from-controller/no-reboot/reboot-time <TIME>/
staggered-reboot/upgrade-time <TIME>)}
```

rf-domain [<RF-DOMAIN-NAME> all containing <WORD> filter location <WORD>]	<p>Upgrades firmware on devices in a specified RF Domain or all RF Domains. Devices within a RF Domain are upgraded through the RF Domain manager.</p> <ul style="list-style-type: none"> • <RF-DOMAIN-NAME> - Upgrades devices in the RF Domain identified by the <RF-DOMAIN-NAME> keyword. • <RF-DOMAIN-NAME> - Specify the RF Domain name. • all - Upgrades devices across all RF Domains • containing <WORD> - Filters RF Domains by their names. RF Domains with names containing the sub-string identified by the <WORD> keyword are filtered. Devices on the filtered RF Domains are upgraded. • filter location <WORD> - Filters devices by their location. All devices with location matching the <WORD> keyword are upgraded.
<DEVICE-TYPE>	<p>After specifying the RF Domain, select the device type. The options are: AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533, RFS 4000, NX 5500, NX 75XX, NX 95XX, NX 96XX, and VX 9000. After specifying the RF Domain and the device type, configure any one of the following actions: force devices to upgrade, or initiate an upgrade through the adopting controller.</p>
<MAC/HOSTNAME>	<p>Optional. Use this option to identify specific devices for upgradation. Specify the device's MAC address or hostname. The device should be within the specified RF Domain and of the specified device type. After identifying the devices to upgrade, configure any one of the following actions: force devices to upgrade, or initiate an upgrade through the adopting controller.</p> <p>Note: If no MAC address or hostname is specified, all devices of the type selected are upgraded.</p>
force	<p>Optional. Select this option to force upgrade for the selected device(s). When selected, the devices are upgraded even if they have the same firmware as the upgrading access point, wireless controller, or service platform. If forcing a device upgrade, optionally specify any one of the following options: no-reboot, reboot-time, upgrade-time, or reboot-time.</p>
from-controller	<p>Optional. Upgrades a device through the adopted device. If initiating an upgrade through the adopting controller, optionally specify any one of the following options: no-reboot, reboot-time, upgrade-time, or reboot-time.</p>
no-reboot {staggered-reboot}	<p>Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)</p>
reboot-time <TIME> {staggered-reboot}	<p>Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.</p>
staggered-reboot	<p>This keyword is common to all of the above. Optional. Enables staggered reboot (one at a time) without network impact</p>
upgrade-time <TIME> {no-reboot reboot-time <TIME>}	<p>Optional. Schedules an automatic firmware upgrade</p> <ul style="list-style-type: none"> • <TIME> - Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format. After a scheduled upgrade, the following actions can be performed. <ul style="list-style-type: none"> • no-reboot - Optional. Disables automatic reboot after a successful upgrade the device must be manually restarted) • reboot-time <TIME> - Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.

Example (User Exec Mode)

```
NOC-NX9500>show adoption status
```

```
-----  
-----
```

DEVICE-NAME UPTIME	VERSION	CFG-STAT	SGS	ADOPTED-BY	LAST-ADOPTION
nx7500-3D1F06 22:32:38	5.9.2.0-004D	version-mismatch	No	NOC-NX9500	2 days 12:23:52
t5-ED7C6C 22:33:25	5.4.2.0-010R	configured	No	NOC-NX9500	13 days 22:47:46

 Total number of devices displayed: 2
 NOC-NX9500>
 NOC-NX9500>show device-upgrade versions

CONTROLLER	DEVICE-TYPE	VERSION
NOC-NX9500	ap621	none
NOC-NX9500	ap622	5.9.2.0-005D
NOC-NX9500	ap650	none
NOC-NX9500	ap6511	none
NOC-NX9500	ap6521	none
NOC-NX9500	ap6522	5.9.2.0-005D
NOC-NX9500	ap6532	none
NOC-NX9500	ap6562	5.9.2.0-005D
NOC-NX9500	ap71xx	5.9.2.0-005D
NOC-NX9500	ap7502	5.9.2.0-005D
NOC-NX9500	ap7522	5.9.2.0-005D
NOC-NX9500	ap7532	5.9.2.0-005D
NOC-NX9500	ap7562	5.9.2.0-005D
NOC-NX9500	ap7602	5.9.2.0-005D
NOC-NX9500	ap7612	5.9.2.0-005D
NOC-NX9500	ap7622	5.9.2.0-005D
NOC-NX9500	ap7632	5.9.2.0-005D
NOC-NX9500	ap7662	5.9.2.0-005D
NOC-NX9500	ap81xx	5.9.2.0-005D
NOC-NX9500	ap82xx	none
NOC-NX9500	ap8432	5.9.2.0-005D
NOC-NX9500	ap8533	5.9.2.0-005D
NOC-NX9500	nx45xx	none
NOC-NX9500	nx5500	none
NOC-NX9500	nx65xx	none
NOC-NX9500	nx75xx	none
NOC-NX9500	nx9000	none
NOC-NX9500	rfs4000	5.9.2.0-005D
NOC-NX9500	rfs6000	none
NOC-NX9500	rfs7000	none
NOC-NX9500	vx9000	none

 NOC-NX9500>
 NOC-NX9500#**device-upgrade load-image nx75xx**
ftp://anonymous:anonymous@192.168.13.10/LatestBuilds/W592/NX7500-LEAN-5.9.0.2-005D

ONTROLLER	STATUS	MESSAGE
NOC-NX9500	Success	Successfully initiated load image

 NOC-NX9500#
 NOC-NX9500#show device-upgrade load-image-status
 Download of nx7500 firmware file is complete
 NOC-NX9500#
 NOC-NX9500>show device-upgrade versions

CONTROLLER	DEVICE-TYPE	VERSION
------------	-------------	---------

```

-----
NOC-NX9500          ap621              none
NOC-NX9500          ap622              5.9.2.0-005D
NOC-NX9500          ap650              none
NOC-NX9500          ap6511            none
NOC-NX9500          ap6521            none
NOC-NX9500          ap6522            5.9.2.0-005D
NOC-NX9500          ap6532            none
NOC-NX9500          ap6562            5.9.2.0-005D
NOC-NX9500          ap71xx            5.9.2.0-005D
NOC-NX9500          ap7502            5.9.2.0-005D
NOC-NX9500          ap7522            5.9.2.0-005D
NOC-NX9500          ap7532            5.9.2.0-005D
NOC-NX9500          ap7562            5.9.2.0-005D
NOC-NX9500          ap7602            5.9.2.0-005D
NOC-NX9500          ap7612            5.9.2.0-005D
NOC-NX9500          ap7622            5.9.2.0-005D
NOC-NX9500          ap7632            5.9.2.0-005D
NOC-NX9500          ap7662            5.9.2.0-005D
NOC-NX9500          ap81xx            5.9.2.0-005D
NOC-NX9500          ap82xx            none
NOC-NX9500          ap8432            5.9.2.0-005D
NOC-NX9500          ap8533            5.9.2.0-005D
NOC-NX9500          nx45xx            none
NOC-NX9500          nx5500            none
NOC-NX9500          nx65xx            none
NOC-NX9500          nx75xx            5.9.2.0-005D
NOC-NX9500          nx9000            none
NOC-NX9500          rfs4000           5.9.2.0-005D
NOC-NX9500          rfs6000           none
NOC-NX9500          rfs7000           none
NOC-NX9500          vx9000            none
-----

```

```

NOC-NX9500>
NOC-NX9500>device-upgrade nx7500-3D1F06
-----

```

CONTROLLER	STATUS	MESSAGE
B4-C7-99-6C-88-09	Success	Queued 1 devices to upgrade

```

NOC-NX9500>
NOC-NX9500>show device-upgrade status
Number of devices currently being upgraded : 1
Number of devices waiting in queue to be upgraded : 0
Number of devices currently being rebooted : 0
Number of devices waiting in queue to be rebooted : 0
Number of devices failed upgrade : 0
-----

```

DEVICE	STATE	UPGRADE TIME	REBOOT TIME	PROGRESS	RETRIES	LAST UPDATE
nx7500-3D1F06	downloading	immediate	immediate	17	0	-

```

NOC-NX9500>
-----

```

Example (Privi Exec Mode)

```

nx9500-6C874D#device-upgrade rfs4000-229D58
-----

```

CONTROLLER	STATUS	MESSAGE
------------	--------	---------

```

-----
B4-C7-99-6C-87-4D          Success          Queued 1 devices to upgrade
-----
nx9500-6C874D#show device-upgrade status
Number of devices currently being upgraded : 0
Number of devices waiting in queue to be upgraded : 1
Number of devices currently being rebooted : 0
Number of devices waiting in queue to be rebooted : 0
Number of devices failed upgrade : 0
-----
-----
      DEVICE          STATE    UPGRADE TIME  REBOOT TIME  PROGRESS  RETRIES  LAST UPDATE  ERROR
UPGRADED BY
-----
      rfs4000-229D58  waiting  immediate    immediate    0         0         -
nx9500-6C874D
-----
nx9500-6C874D#

```

disable

This command can be executed in the Priv Exec Mode only. This command turns off (disables) the privileged mode command set and returns you to the User Executable Mode. The prompt changes from *nx9500-6C8809#* to *nx9500-6C8809>*.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

`disable`

Parameters

None

Examples

```

nx9500-6C8809#disable
nx9500-6C8809>

```

enable

Turns on (enables) the privileged mode command set. The prompt changes from *nx9500-6C8809>* to *nx9500-6C8809#*. This command does not do anything in the Privilege Executable mode.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

enable

Parameters

None

Examples

```
nx9500-6C8809>enable
nx9500-6C8809#
```

file-sync (user and privi exec modes)

Syncs trustpoint and/or EAP-TLS X.509 (PKCS#12) certificate between the staging-controller and adopted access points.

When enabling file syncing, consider the following points:

- The X.509 certificate needs synchronization only if the access point is configured to use EAP-TLS authentication.
- Execute the command on the controller adopting the access points.
- Ensure that the X.509 certificate file is installed on the controller.

Syncing of trustpoint/wireless-bridge certificate can be automated. To automate file syncing, in the controller's device/profile configuration mode, execute the following command: **file-sync [auto|count <1-20>]**. For more information, see [file-sync](#) on page 999.



Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
file-sync [cancel|load-file|trustpoint|wireless-bridge]
file-sync cancel [trustpoint|wireless-bridge]
file-sync cancel [trustpoint|wireless-bridge] [<DEVICE-NAME>|all|rf-domain [<DOMAIN-NAME>|all]]
file-sync load-file [trustpoint|wireless-bridge]
file-sync load-file [trustpoint <TRUSTPOINT-NAME>|wireless-bridge] <URL>
file-sync [trustpoint <TRUSTPOINT-NAME>|wireless-bridge] [<DEVICE-NAME>|all|rf-domain [<DOMAIN-NAME>|all]] {from-controller} {reset-radio/upload-time <TIME>}
```

Parameters

```
file-sync cancel [trustpoint|wireless-bridge] [<DEVICE-NAME>|all|rf-domain [<DOMAIN-NAME>|all]]
```

```
file-sync cancel [trustpoint|
wireless-bridge] [<DEVICE-
NAME>| all|rf-domain
[<DOMAIN-NAME>| all]]
```

Cancels scheduled file synchronization

- trustpoint – Cancels scheduled trustpoint synchronization on a specified AP, all APs, or APs within a specified RF Domain
- wireless-bridge – Cancels scheduled wireless-bridge certificate synchronization on a specified AP, all APs, or APs within a specified RF Domain
 - <DEVICE-NAME> – Cancels scheduled trustpoint/certificate synchronization on a specified AP. Specify the AP's hostname or MAC address.
 - all – Cancels scheduled trustpoint/certificate synchronization on all APs
 - rf-domain [<DOMAIN-NAME>|all] – Cancels scheduled trustpoint/certificate synchronization on all APs in a specified RF Domain or in all RF Domains
 - <DOMAIN-NAME> – Cancels scheduled trustpoint/certificate synchronization on all APs within a specified RF Domain. Specify the RF Domain's name.
 - all – Cancels scheduled trustpoint/certificate synchronization on all RF Domains

```
file-sync load-file [trustpoint|wireless-bridge] <URL>
```

```
file-sync load-file [trustpoint|
wireless-bridge] <URL>
```

Loads the following files on to the staging controller:

- trustpoint – Loads the trustpoint, including CA certificate, server certificate and private key
- wireless-bridge – Loads the wireless-bridge certificate to the staging controller. Use this command to load the certificate to the controller before scheduling or initiating a certificate synchronization.
- <URL> – Provide the trustpoint/certificate location using one of the following formats:

```
tftp://<hostname|IP>[:port]/path/file
```

```
ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file
```

```
sftp://<user>:<passwd>@<hostname|IP>[:port]/path/file
```

```
http://<hostname|IP>[:port]/path/file
```

Note: Both IPv4 and IPv6 address types are supported.

```
cf:/path/file
```

```
usb<n>:/path/file
```

```
file-sync [trustpoint <TRUSTPOINT-NAME>|wireless-bridge] [<DEVICE-NAME>|
all|rf-domain [<DOMAIN-NAME>|all]] {from-controller} {reset-radio|upload-time <TIME>}
```

<pre>file-sync trustpoint <TRUSTPOINT-NAME> [<DEVICE-NAME>] all rf- domain [<DOMAIN-NAME> all] from-controller]</pre>	<p>Configures file-syncing parameters</p> <ul style="list-style-type: none"> trustpoint <TRUSTPOINT-NAME> - Syncs a specified trustpoint between controller and its adopted APs <ul style="list-style-type: none"> <TRUSTPOINT-NAME> - Specify the trustpoint name. wireless-bridge - Syncs wireless-bridge certificate between controller and its adopted APs <p>After specifying the file that is to be synced, configure following file-sync parameters:</p> <ul style="list-style-type: none"> <DEVICE-NAME> - Syncs trustpoint/certificate with a specified AP. Specify the AP's hostname or MAC address. all - Syncs trustpoint/certificate with all APs rf-domain [<DOMAIN-NAME> all] from-controller - Syncs trustpoint/certificate with all APs in a specified RF Domain or in all RF Domains <ul style="list-style-type: none"> <DOMAIN-NAME> - Select to sync with APs within a specified RF Domain. Specify the RF Domain's name. all - Select to sync with APs across all RF Domains <p>from-controller - Optional. Loads certificate to the APs from the adopting controller and not the RF Domain manager</p> <p>After specifying the access points, specify the following options: reset-radio and upload-time.</p>
<pre>reset-radio</pre>	<p>This keyword is recursive and applicable to all of the above parameters. Optional. Resets the radio after file synchronization. Reset the radio in case the certificate is renewed along with no changes made to the 'bridge EAP username' and 'bridge EAP password'.</p>
<pre>upload-time <TIME></pre>	<p>This keyword is recursive and applicable to all of the above parameters.</p> <ul style="list-style-type: none"> upload-time - Optional. Schedules certificate upload at a specified time <ul style="list-style-type: none"> <TIME> - Specify the time in the MM/DD/YYYY-HH:MM or HH:MM format. If no time is configured, the process is initiated as soon as the command is executed.

Example (User Exec Mode)

```
NOC-NX9500>file-sync wireless-bridge ap7161-11E6C4 upload-time 06/01/2018-12:30
```

CONTROLLER	STATUS	MESSAGE
B4-C7-99-6C-88-09	Success	Queued 1 APs to upload

```
NOC-NX9500>
```

The following command uploads certificate to all access points:

```
NOC-NX9500>file-sync wireless-bridge all upload-time 06/01/2018-23:42
```

Example (Privi Exec Mode)

```
rfs4000-6DB5D4#file-sync wireless-bridge ap7161-11E6C4 upload-time 06/01/2018-12:30
```

CONTROLLER	STATUS	MESSAGE
B4-C7-99-6D-B5-D4	Success	Queued 1 APs to upload

```
rfs4000-6DB5D4#
```


The following command uploads certificate to all access points:

```
rfs4000-6DB5D4#file-sync wireless-bridge all upload-time 06/01/2018-23:42
```

join-cluster (user and privi exec modes)

Adds a device (access point, wireless controller, or service platform), as a member, to an existing cluster of devices. Assign a static IP address to the device before adding to a cluster. Note, a cluster can be only formed of devices of the same model type.



Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
join-cluster <IP> user <USERNAME> password <WORD> { level | mode }  
join-cluster <IP> user <USERNAME> password <WORD> { level [1|2] | mode [active|standby] }
```

Parameters

```
join-cluster <IP> user <USERNAME> password <WORD> { level [1|2] | mode [active|standby] }
```

join-cluster	Adds a access point wireless controller, or service platform to an existing cluster
<IP>	Specify the cluster member's IP address.
user <USERNAME>	Specify a user account with super user privileges on the new cluster member
password <WORD>	Specify password for the account specified in the user parameter
level [1 2]	Optional. Configures the routing level <ul style="list-style-type: none">• 1 - Configures level 1 routing• 2 - Configures level 2 routing
mode [active standby]	Optional. Configures the cluster mode <ul style="list-style-type: none">• active - Configures this cluster as active• standby - Configures this cluster to be on standby mode

Usage Guidelines

To add a device to an existing cluster:

- Configure a static IP address on the device (access point, wireless controller, or service platform).
- Provide username and password for superuser, network admin, system admin, or operator accounts.

After adding a device to a cluster, execute the "write memory" command to ensure the configuration persists across reboots.

Examples (User Exec Mode)

```
rfs4000-229D58>join-cluster 192.168.13.15 user admin password superuser level 1  
mode standby  
... connecting to 192.168.13.15  
... applying cluster configuration
```

```

... committing the changes
... saving the changes
[OK]
rfs4000-229D58>
rfs4000-229D58>show context
!
! Configuration of RFS4000 version 5.9.2.0-012D
!
!
version 2.5
!
!
.....
cluster name TechPubs
cluster mode standby
cluster member ip 192.168.13.15 level 1
logging on
logging console warnings
logging buffered warnings
!
!
end
rfs4000-229D58>

```

Example (Privi Exec Mode)

```

rfs4000-6DB5D4#join-cluster 192.168.13.16 user admin password superuser level 1
mode standby
... connecting to 192.168.13.16
... applying cluster configuration
... committing the changes
... saving the changes
[OK]
rfs4000-6DB5D4#
rfs4000-6DB5D4#show context
!
! Configuration of RFS6000 version 5.9.2.0-012D
!
!
version 2.5
!
!
.....
cluster name TechPubs
cluster mode standby
cluster member ip 192.168.13.16 level 1
logging on
logging console warnings
logging buffered warnings
!
!
end
rfs4000-6DB5D4#

```

Related Commands

create-cluster (user and privi exec modes) on page 47	Creates a new cluster on the specified device
cluster (user and privi exec modes) on page 46	Initiates cluster context. The cluster context enables centralized management and configuration of all cluster members from any one member.

l2tpv3 (user and privi exec modes)

Establishes or brings down a *Layer 2 Tunnel Protocol Version 3* (L2TPV3) tunnel



Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
l2tpv3 tunnel [<TUNNEL-NAME>|all]
l2tpv3 tunnel <TUNNEL-NAME> [down|session|up]
l2tpv3 tunnel <TUNNEL-NAME> [down|up] {on <DEVICE-NAME>}
l2tpv3 tunnel <TUNNEL-NAME> session <SESSION-NAME> [down|up] {on <DEVICE-NAME>}
l2tpv3 tunnel all [down|up] {on <DEVICE-NAME>}
```

Parameters

```
l2tpv3 tunnel <TUNNEL-NAME> [down|up] {on <DEVICE-NAME>}
```

l2tpv3 tunnel	Establishes or brings down L2TPV3 tunnels
<TUNNEL-NAME> [down up]	Specifies the tunnel name to establish or bring down <ul style="list-style-type: none">• down - Brings down the specified tunnel• up - Establishes the specified tunnel
on <DEVICE-NAME>	Optional. Establishes or brings down a tunnel on a specified device <ul style="list-style-type: none">• <DEVICE-NAME> - Specify the name of the AP, wireless controller, or service platform.

```
l2tpv3 tunnel <TUNNEL-NAME> session <SESSION-NAME> [down|up] {on <DEVICE-NAME>}
```

l2tpv3 tunnel	Establishes or brings down L2TPV3 tunnels
<TUNNEL-NAME> [session <SESSION-NAME>] [down up]	Establishes or brings down a specified session inside an L2TPV3 tunnel <ul style="list-style-type: none">• <TUNNEL-NAME> - Specify the tunnel name.• session <SESSION-NAME> - Identifies a specific session<ul style="list-style-type: none"><SESSION-NAME> - Specify the session name.down - Brings down the session identified by the <SESSION-NAME> keywordup - Establishes the session identified by the <SESSION-NAME> keyword
on <DEVICE-NAME>	Optional. Establishes or brings down a tunnel session on a specified device <ul style="list-style-type: none">• <DEVICE-NAME> - Specify the name of the AP, wireless controller, or service platform.

```
l2tpv3 tunnel all [down|up] {on <DEVICE-NAME>}
```

l2tpv3 tunnel	Establishes or brings down L2TPV3 tunnel
all [down up]	Establishes or brings down all L2TPV3 tunnels <ul style="list-style-type: none"> • down – Brings down all tunnels • up – Establishes all tunnels
on <DEVICE-NAME>	Optional. Establishes or brings down all tunnels on a specified device <ul style="list-style-type: none"> • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Examples (User Exec Mode)

```
nx9500-6C8809>l2tpv3 tunnel Tunnel1 session Tunnel1Session1 up on nx9500-6C8809
```

Example (Privi Exec Mode)

```
nx9500-6C8809#l2tpv3 tunnel TestTunnel session TestTunnelSession1 up on rfs4000-6DB5D4
```



Note

For more information on the L2TPV3 tunnel configuration mode and commands, see [L2TPV3-POLICY](#).

logging (user and privi exec modes)

Modifies message logging settings



Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
logging monitor {<0-7>|alerts|critical|debugging|emergencies|errors|informational|
notifications|warnings}
```

Parameters

```
logging monitor {<0-7>|alerts|critical|debugging|emergencies|errors|informational|
notifications|warnings}
```

monitor Sets the terminal lines logging levels. The logging severity levels can be set from 0 - 7. The system configures default settings, if no logging severity level is specified.

- <0-7> - Optional. Specify the logging severity level from 0-7. The various levels and their implications are as follows:
- alerts - Optional. Immediate action needed (severity=1)
- critical - Optional. Critical conditions (severity=2)
- debugging - Optional. Debugging messages (severity=7)
- emergencies - Optional. System is unusable (severity=0)
- errors - Optional. Error conditions (severity=3)
- informational - Optional. Informational messages (severity=6)
- notifications - Optional. Normal but significant conditions (severity=5)
- warnings - Optional. Warning conditions (severity=4)

Note: Before configuring the message logging level, ensure logging module is enabled. To enable message logging, in the device's configuration mode, execute the logging > on command. Message logging can also be enabled on a profile. All devices using the profile will have message logging enabled.

Example (User Exec Mode)

```
NOC-NX9500(config-device-B4-C7-99-6C-88-09)#logging on
NOC-NX9500>logging monitor debugging
NOC-NX9500>show logging
```

```
Logging module: enabled
  Aggregation time: disabled
  Console logging: level debugging
  Monitor logging: level debugging
  Buffered logging: level warnings
  Syslog logging: level warnings
  Facility: local7
```

Log Buffer (2208029 bytes):

```
Jan 03 06:48:40 2018: NOC-NX9500 : %NSM-4-IFUP: Interface gel is up
Jan 03 06:48:39 2018: NOC-NX9500 : %NSM-4-IFUP: Interface gel is up
Jan 03 06:48:37 2018: NOC-NX9500 : %NSM-4-IFDOWN: Interface gel is down
Jan 03 06:48:36 2018: NOC-NX9500 : %NSM-4-IFUP: Interface gel is up
Jan 02 03:41:56 2018: NOC-NX9500 : %NSM-4-IFUP: Interface ge3 is up
Jan 02 03:41:55 2018: NOC-NX9500 : %NSM-4-IFUP: Interface ge3 is up
Jan 02 03:41:53 2018: NOC-NX9500 : %NSM-4-IFDOWN: Interface ge3 is down
Jan 02 03:41:22 2018: NOC-NX9500 : %NSM-4-IFUP: Interface ge3 is up
Jan 02 03:41:20 2018: NOC-NX9500 : %NSM-4-IFUP: Interface ge3 is up
```

```
--More--
NOC-NX9500>
```

Example (Priv Exec Mode)

```
nx9500-6C8809#logging monitor warnings
nx9500-6C8809#
rfs4000-229D58#logging monitor 2
rfs4000-229D58#
```

Related Commands

no (user exec mode) on page 83	Resets terminal lines logging levels
no (priv-exec-mode) on page 189	

mint (user and privi exec modes)

Uses MiNT protocol to perform a ping and trace route to a remote device



Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
mint [ping|traceroute]
mint ping <MINT-ID> {(count <1-10000>/size <1-64000>/timeout <1-10>)}
mint traceroute <MINT-ID> {(destination-port <1-65535>/max-hops <1-255>/
source-port <1-65535>/timeout <1-255>)}
```

Parameters

```
mint ping <MINT-ID> {(count <1-10000>/size <1-64000>/timeout <1-10>)}
```

ping <MINT-ID>	Sends a MiNT echo message to a specified destination <ul style="list-style-type: none">• <MINT-ID> - Specify the destination device's MiNT ID.
count <1-10000>	Optional. Sets the number of ping packets sent to the specified MiNT destination <ul style="list-style-type: none">• <1-60> - Specify a value from 1 - 10000. The default is 3.
size <1-64000>	Optional. Sets the MiNT payload size in bytes <ul style="list-style-type: none">• <1-64000> - Specify a value from 1 - 640000. The default is 64 bytes.
timeout <1-10>	Optional. Sets a response time in seconds <ul style="list-style-type: none">• <1-10> - Specify a value from 1 sec - 10 sec. The default is 1 second.

```
mint traceroute <MINT-ID> {(destination-port <1-65535>/max-hops <1-255>/
source-port <1-65535>/timeout <1-255>)}
```

traceroute <MINT-ID>	Prints the route packets trace to a device <ul style="list-style-type: none">• <MINT-ID> - Specify the destination device's MiNT ID.
destination-port <1-65535>	Optional. Sets the <i>Equal-cost Multi-path</i> (ECMP) routing destination port <ul style="list-style-type: none">• <1-65535> - Specify a value from 1 - 65535. The default port is 45.
max-hops <1-255>	Optional. Sets the maximum number of hops a traceroute packet traverses in the forward direction <ul style="list-style-type: none">• <1-255> - Specify a value from 1 - 255. The default is 30.
source-port <1-65535>	Optional. Sets the ECMP source port <ul style="list-style-type: none">• <1-65535> - Specify a value from 1 - 65535. The default port is 45.
timeout <1-255>	Optional. Sets the minimum response time period in seconds <ul style="list-style-type: none">• <1-65535> - Specify a value from 1 sec - 255 sec. The default is 30 seconds.

Example (User Exec Mode)

```
NOC-NX9500>mint ping 4D.83.30.A4
MiNT ping 4D.83.30.A4 with 64 bytes of data.
  Response from 4D.83.30.A4: id=16777216 time=0.262 ms
  Response from 4D.83.30.A4: id=33554432 time=2.025 ms
  Response from 4D.83.30.A4: id=50331648 time=0.256 ms

--- 4D.83.30.A4 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.256/0.848/2.025 ms
NOC-NX9500>
```

Example (Privi Exec Mode)

```
rfs4000-229D58#mint ping 68.88.0D.A7
MiNT ping 68.88.0D.A7 with 64 bytes of data.
  Response from 68.88.0D.A7: id=1 time=0.364 ms
  Response from 68.88.0D.A7: id=2 time=0.333 ms
  Response from 68.88.0D.A7: id=3 time=0.368 ms

--- 68.88.0D.A7 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.333/0.355/0.368 ms
rfs4000-229D58#
```

no (user exec mode)

Use the `no` command to remove a setting or to revert a setting to its default value.



Note

The commands have their own set of parameters that can be reset.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
no [adoption|captive-portal|crypto|debug|logging|page|service|terminal|virtual-machine|
wireless]
no adoption {on <DEVICE-OR-DOMAIN-NAME>}
no captive-portal client [captive-portal <CAPTIVE-PORTAL-NAME>|mac <MAC>] {on <DEVICE-OR-
DOMAIN-NAME>}
no crypto pki [server|trustpoint]
no crypto pki [server|trustpoint] <TRUSTPOINT-NAME> {del-key {on <DEVICE-NAME>}/on <DEVICE-
NAME>}
no logging monitor
no page
no service [block-adopter-config-update|locator|snmp|ssm|wireless]
no service snmp sysoid wing5
no service block-adopter-config-update
no service ssm trace pattern {<WORD>} {on <DEVICE-NAME>}
no service wireless [trace pattern {<WORD>} {on <DEVICE-NAME>}|
unsanctioned ap air-terminate <BSSID> {on <DOMAIN-NAME>}]
no service locator {on <DEVICE-NAME>}
no terminal [length|width]
no virtual-machine assign-usb-ports {on <DEVICE-NAME>}
no wireless client [all|<MAC>]
no wireless client all {filter/on}
no wireless client all {filter [wlan <WLAN-NAME>]}
no wireless client all {on <DEVICE-OR-DOMAIN-NAME>} {filter [wlan <WLAN-NAME>]}
no wireless client mac <MAC> {on <DEVICE-OR-DOMAIN-NAME>}
```

Parameters

no <PARAMETERS>

no <PARAMETERS>	Resets or reverts settings based on the parameters passed
-----------------	---

Usage Guidelines

The *no* command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Examples

```
nx9500-6C8809>no adoption
nx9500-6C8809>no page
nx9500-6C8809>no service cli-tables-expand line
```

on (user and privi exec modes)

Executes the following commands in the RF Domain context: *clrscr*, *do*, *end*, *exit*, *help*, *service*, and *show*

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
on rf-domain [<RF-DOMAIN-NAME>|all]
```


Parameters

```
on rf-domain [<RF-DOMAIN-NAME>|all]
```

on rf-domain [<RF-DOMAIN-NAME> all]	Enters the RF Domain context based on the parameter specified <ul style="list-style-type: none">• <RF-DOMAIN-NAME> - Specify the RF Domain name. Enters the specified RF Domain context.• all - Specifies all RF Domains.
-------------------------------------	--

Example (User Exec Mode)

```
nx9500-6C8809>on rf-domain TechPubs
nx9500-6C8809(TechPubs)>?
on RF-Domain Mode commands:
```

```
clrscr  Clears the display screen
do      Run commands from Exec mode
end     End current mode and change to EXEC mode
exit   End current mode and down to previous mode
help   Description of the interactive help system
service Service Commands
show   Show running system information
```

```
nx9500-6C8809(TechPubs)>
nx9500-6C8809(rf-domain-all)>?
on RF-Domain Mode commands:
```

```
clrscr  Clears the display screen
do      Run commands from Exec mode
end     End current mode and change to EXEC mode
exit   End current mode and down to previous mode
help   Description of the interactive help system
service Service Commands
show   Show running system information
```

```
nx9500-6C8809(rf-domain-all)>
```

Example (Privi Exec Mode)

```
nx9500-6C8809#on rf-domain TechPubs
nx9500-6C8809(TechPubs)#
NOC-NX9500#on rf-domain default
NOC-NX9500(default)#?
on RF-Domain Mode commands:
```

```
clrscr  Clears the display screen
do      Run commands from Exec mode
end     End current mode and change to EXEC mode
exit   End current mode and down to previous mode
help   Description of the interactive help system
service Service Commands
show   Show running system information
```

```
NOC-NX9500(default)#
```

```
NOC-NX9500(default)#show sessions on RFS6K-SITE1-VLAN20
```

INDEX	COOKIE	NAME	START TIME	FROM	ROLE
1	10	admin	2018-01-02 04:31:41	Console	superuser
2	3	snmp	2018-01-02 03:39:59	127.0.0.1	superuser
3	4	snmp2	2018-01-02 03:39:59	127.0.0.1	superuser

```
NOC-NX9500(default)#
```

opendns (user and privi exec modes)

Fetches the OpenDNS device_id from the OpenDNS site. Use this command to fetch the OpenDNS device_id. Once fetched, apply the device_id to WLANs that are to be OpenDNS enabled.

OpenDNS is a free DNS service that enables swift Web navigation without frequent outages. It is a reliable DNS service that provides the following services: DNS query resolution, Web-filtering, protection against virus and malware attacks, performance enhancement, etc.

This command is part of a set of configurations that are required to integrate WiNG devices with OpenDNS. When integrated, DNS queries going out of the WiNG device (access point, controller, or service platform) are re-directed to OpenDNS (208.67.220.220 or 208.67.222.222) resolvers that act as proxy DNS servers.

For more information on integrating WiNG devices with OpenDNS site, see [Example: Enabling OpenDNS Support](#) on page 87.



Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
opendns [APIToken|username]
opendns APIToken <OPENDNS-APITOKEN>
opendns username <USERNAME> password <OPENDNS-PSWD> label <LABEL>
```



Note

Note, as per the current implementation both of the above commands can be used to fetch the device_id from the OpenDNS site.

Parameters

```
opendns APIToken <OPENDNS-APITOKEN>
```

opendns	Fetches the device_id from the OpenDNS site using the OpenDNS API token
APIToken <OPENDNS-APITOKEN>	Configures the OpenDNS APIToken. This is the token provided you by CISCO at the time of subscribing for their OpenDNS service. <ul style="list-style-type: none">• <OPENDNS-APITOKEN> - Provide the OpenDNS API token (should be a valid token). For every valid OpenDNS API token provided a device_id is returned. Apply this device_id to WLANs that are to be OpenDNS enabled. Once applied, DNS queries originating from associating clients are appended with an additional 31 bytes of data (representing the device ID) at the end of the DNS packet. For information on configuring the device_id in the WLAN context, see opendns on page 586.

```
opendns username <USERNAME> password <OPENDNS-PSWD> label <LABEL>
```

opendns	Fetches the device_id from the OpenDNS site using the OpenDNS credentials
username <USERNAME>	Configures the OpenDNS user name. This is your OpenDNS email ID provided by CISCO at the time of subscribing for their OpenDNS service. <ul style="list-style-type: none"> <USERNAME> - Provide the OpenDNS user name (should be a valid OpenDNS username).
password <OPENDNS-PSWD>	Configures the password associated with the user name specified in the previous step <ul style="list-style-type: none"> <OPENDNS-PSWD> - Provide the OpenDNS password (should be a valid OpenDNS password).
label <LABEL>	Configures the network label. This the label (the user friendly name) of your network, and should be the same as the label (name) configured on the OpenDNS portal. <ul style="list-style-type: none"> <LABEL> - Specify your network label. <p>For every set of user name, password, and label passed only one unique device_id is returned. Apply this device_id to WLANs that are to be OpenDNS enabled. Once applied, DNS queries originating from associating clients are appended with an additional 31 bytes of data (representing the device ID) at the end of the DNS packet. For information on configuring the device_id in the WLAN context, see opendns on page 586.</p>

Usage Guidelines

Use your OpenDNS credentials to logon to the opendns.org site and use the labels, edit settings, and customize content filtering options to configure Web filtering settings.

Example

```
ap7161-E6D512>opendns username bob@examplecompany.com password opendns label company_name
Connecting to OpenDNS server...
device_id = 0014AADF8EDC6C59
ap7161-E6D512>
nx9600-7F3C7F>opendns ApiToken 9110B39543DEB2ECA1F473AE03E8899C00019073 device_id =
001480fe36dcb245
nx9600-7F3C7F>
```

Example: Enabling OpenDNS Support

The following example shows how to enable OpenDNS support:

- 1 Fetch the OpenDNS device_id from the OpenDNS site.
 - a In the User/Privilege executable mode execute one of the following commands:

```
nx9500-6C8809#opendns APIToken <OPENDNS-APITOKEN>
nx9500-6C8809#opendns ApiToken 9110B39543DEB2ECA1F473AE03E8899C00019073
device_id = 001480fe36dcb245nx9500-6C8809#
```

OR

```
nx9500-6C8809#opendns username <USERNAME> password <OPENDNS-PSWD> label <LABEL>
```



Note

The *OpenDNS API token* and/or *user account credentials* are provided the OpenDNS service provider when subscribing for the OpenDNS service.

- b Apply the device_id fetched in the step 1 to the WLAN.

```
nx9500-6C8809(config-wlan-opendns)#opendns device-id <OPENDNS-DEVICE-ID>
nx9500-6C8809(config-wlan-opendns)#opendns device-id 001480fe36dcb245
nx9500-6C8809(config-wlan-opendns)#show context
wlan opendns
```

```
ssid opendns
bridging-mode local
encryption-type none
authentication-type none
opendns device-id 001480fe36dcb245
nx9500-6C8809(config-wlan-opendns)#
```



Note

Once applied, DNS queries originating from wireless clients associating with the WLAN are appended with an additional 31 bytes of data (representing the device ID) at the end of the DNS packet.

- 2 Configure a DHCP server policy, and set the DHCP pool's DNS server configuration to point to the OpenDNS servers.

```
nx9500-6C8809(config-dhcp-policy-opendns-pool-opendnsPool)#dns-server 208.67.222.222
```



Note

You can configure any one of the following OpenDNS servers: 208.67.222.222 OR 208.67.222.220

```
nx9500-6C8809(config-dhcp-policy-opendns-pool-opendnsPool)#show context
```

```
dhcp-pool opendnsPool  
dns-server 208.67.222.222
```

```
nx9500-6C8809(config-dhcp-policy-opendns-pool-opendnsPool)#
```

- 3 Apply the DHCP server policy configured in step 2 on the access point, controller, or service platform.

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#use dhcp-server-policy opendns
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context include-factory | include
use
use profile default-nx9000
use rf-domain TechPubs
use database-policy default
use nsight-policy noc
use dhcp-server-policy opendns
use auto-provisioning-policy TechPubs
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```



Note

When configured, DNS queries are forwarded by the access point, controller, or service platform to the specified OpenDNS resolver.

- 4 Configure an IP Access Control List with the following permit and deny rules:

```
nx9500-6C8809(config-ip-acl-OpenDNS)#permit udp any host 208.67.222.222 eq dns rule-
precedence 1 rule-description "allow dns queries only to OpenDNS"
```

```
nx9500-6C8809(config-ip-acl-OpenDNS)#deny udp any any eq dns rule-precedence 10 rule-
description "block all DNS queries"
```

```
nx9500-6C8809(config-ip-acl-OpenDNS)#permit ip any any rule-precedence 100 rule-
description "allow all other ip packets"
```

```
nx9500-6C8809(config-ip-acl-OpenDNS)#show context
```

```
ip access-list OpenDNS  
permit udp any host 208.67.222.222 eq dns rule-precedence 1 rule-description "allow dns  
queries only to OpenDNS"  
deny udp any any eq dns rule-precedence 10 rule-description "block all dns queries"
```

```
permit ip any any rule-precedence 100 rule-description "allow all other ip packets"
nx9500-6C8809(config-ip-acl-OpenDNS)#
```



Note

When configured and applied in the WLAN context, the IP ACL prevents wireless clients from adding their own DNS servers to bypass the Web filtering and network policies enforced by OpenDNS.

- 5 Apply the IP ACL configured in step 4 in the WLAN context.
- ```
nx9500-6C8809(config-wlan-opendns)#use ip-access-list out OpenDNS
nx9500-6C8809(config-wlan-opendns)#show context
wlan opendns
 ssid opendns
 vlan 1
 bridging-mode local
 encryption-type none
 authentication-type none
 use ip-access-list in OpenDNS
 use ip-access-list out OpenDNS
 opendns device-id 0014AADF8EDC6C59
nx9500-6C8809(config-wlan-opendns)#
```
- 



#### Note

When applied to the WLAN, only the DNS queries directed to the OpenDNS server are forwarded. All other DNS queries are dropped.

---

*page (user and privi exec modes)*

Toggles a device's paging function. Enabling this option displays the CLI command output page by page, instead of running the entire output at once.

---



#### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

---

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

page

#### Parameters

None

#### Examples (User Exec Mode)

```
rfs4000-6DB5D4#page
rfs4000-6DB5D4#
```

## Example (Privi Exec Mode)

nx9500-6C8809#page  
nx9500-6C8809#

## Related Commands

`no (user exec mode) on` Disables paging  
page 83

`no (priv-exec-mode) on` Disables paging  
page 189

## *ping (user and privi exec modes)*

Sends ICMP (Internet Controller Message Protocol) echo messages to a user-specified location



### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

## Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
ping <IP/HOSTNAME> {count <1-10000>|dont-fragment {count|size}|size <1-64000>|
source [<IP>|pppoe|vlan <1-4094>|wwan]}
```

## Parameters

```
ping <IP/HOSTNAME> {count <1-10000>|dont-fragment {count|size}|size <1-64000>|
source [<IP>|pppoe|vlan <1-4094>|wwan]}
```

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IP/HOSTNAME>              | Specify the destination IP address or hostname. When entered without any parameters, this command prompts for an IP address or a hostname.                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| count <1-10000>            | Optional. Sets the pings to the specified destination <ul style="list-style-type: none"><li>• &lt;1-10000&gt; - Specify a value from 1 - 10000. The default is 5.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                          |
| dont-fragment {count size} | Optional. Sets the don't fragment bit in the ping packet. Packets with the dont-fragment bit specified are not fragmented. When a packet, with the dont-fragment bit specified, exceeds the specified MTU (maximum transmission unit) value, an error message is sent from the device trying to fragment it. <ul style="list-style-type: none"><li>• count &lt;1-10000&gt; - Optional. Sets the pings to the specified destination from 1 - 10000. The default is 5.</li><li>• size &lt;1-64000&gt; - Optional. Sets the ping payload size from 1 - 64000 bytes. The default is 100 bytes.</li></ul> |

|                                                |                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| size <1-64000>                                 | Optional. Sets the ping payload size in bytes <ul style="list-style-type: none"> <li>&lt;1-64000&gt; - Specify the ping payload size from 1 - 64000. The default is 100 bytes.</li> </ul>                                                                                                                                                                                                                   |
| source [<IP>]<br>pppoe  vlan<br><1-4094> wwan] | Optional. Sets the source address or interface name. This is the source of the ICMP packet to the specified destination. <ul style="list-style-type: none"> <li>&lt;IP&gt; - Specifies the source IP address</li> <li>pppoe - Selects the PPP over Ethernet interface</li> <li>vlan &lt;1-4094&gt; - Selects the VLAN interface from 1 - 4094</li> <li>wwan - Selects the wireless WAN interface</li> </ul> |

### Examples (User Exec Mode)

```
NOC-NX9500>ping 10.234.160.13
PING 10.234.160.13 (10.234.160.13) 100(128) bytes of data.
108 bytes from 10.234.160.13: icmp_seq=1 ttl=64 time=3.61 ms
108 bytes from 10.234.160.13: icmp_seq=2 ttl=64 time=0.177 ms
108 bytes from 10.234.160.13: icmp_seq=3 ttl=64 time=0.162 ms
108 bytes from 10.234.160.13: icmp_seq=4 ttl=64 time=0.167 ms
108 bytes from 10.234.160.13: icmp_seq=5 ttl=64 time=0.170 ms

--- 10.234.160.13 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.162/0.857/3.613/1.378 ms
NOC-NX9500>
NOC-NX9500>ping 10.234.160.11 source vlan 1
PING 10.234.160.11 (10.234.160.11) from 10.234.160.5 vlan1: 100(128) bytes of data.
108 bytes from 10.234.160.11: icmp_seq=1 ttl=64 time=6.87 ms
108 bytes from 10.234.160.11: icmp_seq=2 ttl=64 time=0.469 ms
108 bytes from 10.234.160.11: icmp_seq=3 ttl=64 time=0.448 ms
108 bytes from 10.234.160.11: icmp_seq=4 ttl=64 time=0.437 ms
108 bytes from 10.234.160.11: icmp_seq=5 ttl=64 time=0.459 ms

--- 10.234.160.11 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
rtt min/avg/max/mdev = 0.437/1.738/6.879/2.570 ms
NOC-NX9500>
```

### Examples (Priv Exec Mode)

```
rfs4000-229D58#ping 10.233.89.182 source vlan 1
PING 10.233.89.182 (10.233.89.182) from 192.168.13.24 vlan1: 100(128) bytes of data.
From 192.168.13.2 icmp_seq=1 Packet filtered
From 192.168.13.2 icmp_seq=2 Packet filtered
From 192.168.13.2 icmp_seq=3 Packet filtered
From 192.168.13.2 icmp_seq=4 Packet filtered
From 192.168.13.2 icmp_seq=5 Packet filtered

--- 10.233.89.182 ping statistics ---
5 packets transmitted, 0 received, +5 errors, 100% packet loss, time 3997ms

rfs4000-229D58#
```

### ping6 (user and privi exec modes)

Sends ICMPv6 echo messages to a user-specified IPv6 address



#### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

## Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
ping6 <IPv6/HOSTNAME> {<INTF-NAME>} {(count <1-10000>|size <1-64000>)}
```

## Parameters

```
ping6 <IPv6/HOSTNAME> {<INTF-NAME>} {(count <1-10000>|size <1-64000>)}
```

|                 |                                                                                                                                                                                                |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IPv6/HOSTNAME> | Specify the destination IPv6 address or hostname.                                                                                                                                              |
| <INTF-NAME>     | Specify the interface name for link local/broadcast address                                                                                                                                    |
| count <1-10000> | Optional. Sets the pings to the specified IPv6 destination <ul style="list-style-type: none"><li>• &lt;1-10000&gt; - Specify a value from 1 - 10000. The default is 5.</li></ul>               |
| size <1-64000>  | Optional. Sets the IPv6 ping payload size in bytes <ul style="list-style-type: none"><li>• &lt;1-64000&gt; - Specify the ping payload size from 1 - 64000. The default is 100 bytes.</li></ul> |

## Usage Guidelines

To configure a device's IPv6 address, in the VLAN interface configuration mode, use the **ipv6 > address <IPv6-ADDRESS>** command. After configuring the IPv6 address, use the **ipv6 > enable** command to enable IPv6. For more information, see [ipv6](#) on page 1162 (profile config mode).

## Examples (User Exec Mode)

```
rfs4000-1B3596(config-device-00-23-68-1B-35-96-if-ge4)#show ipv6 interface brief

INTERFACE IPV6 MODE IPV6-ADDRESS/MASK TYPE STATUS PROTOCOL

vlan1 True fe80::223:68ff:fe88:da7/64 Link-Local UP up
vlan1 True 2001:10:10:10:10:10:10:1/64 Global-Permanent UP up
vlan2 False UNASSIGNED None UP up

rfs4000-1B3596(config-device-00-23-68-1B-35-96-if-ge4)#
rfs4000-229D58>ping6 2001:10:10:10:10:10:10:1 count 6
PING 2001:10:10:10:10:10:10:1(2001:10:10:10:10:10:10:1) 100 data bytes
108 bytes from 2001:10:10:10:10:10:10:1: icmp_seq=1 ttl=64 time=0.401 ms
108 bytes from 2001:10:10:10:10:10:10:1: icmp_seq=2 ttl=64 time=0.311 ms
108 bytes from 2001:10:10:10:10:10:10:1: icmp_seq=3 ttl=64 time=0.300 ms
108 bytes from 2001:10:10:10:10:10:10:1: icmp_seq=4 ttl=64 time=0.309 ms
108 bytes from 2001:10:10:10:10:10:10:1: icmp_seq=5 ttl=64 time=0.299 ms
108 bytes from 2001:10:10:10:10:10:10:1: icmp_seq=6 ttl=64 time=0.313 ms

--- 2001:10:10:10:10:10:10:1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 6999ms
rtt min/avg/max/mdev = 0.299/0.318/0.401/0.031 ms
rfs4000-229D58>
```

## Examples (Privileged Exec Mode)

```
rfs4000-880DA7#ping6 2001:10:10:10:10:10:10:2 count 6 size 200
PING 2001:10:10:10:10:10:10:2(2001:10:10:10:10:10:10:2) 200 data bytes
```



```

208 bytes from 2001:10:10:10:10:10:10:2: icmp_seq=1 ttl=64 time=0.509 ms
208 bytes from 2001:10:10:10:10:10:10:2: icmp_seq=2 ttl=64 time=0.323 ms
208 bytes from 2001:10:10:10:10:10:10:2: icmp_seq=3 ttl=64 time=0.318 ms
208 bytes from 2001:10:10:10:10:10:10:2: icmp_seq=4 ttl=64 time=0.317 ms
208 bytes from 2001:10:10:10:10:10:10:2: icmp_seq=5 ttl=64 time=0.314 ms
208 bytes from 2001:10:10:10:10:10:10:2: icmp_seq=6 ttl=64 time=0.318 ms

--- 2001:10:10:10:10:10:10:2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4999ms
rtt min/avg/max/mdev = 0.314/0.349/0.509/0.075 ms
rfs4000-880DA7#

```

*ssh* (user and privi exec modes)

Opens a SSH (Secure Shell) connection between two network devices



#### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
ssh <IP/HOSTNAME> <USER-NAME> {<INF-NAME/LINK-LOCAL-ADD>}
```

#### Parameters

```
ssh <IP/HOSTNAME> <USER-NAME> {<INF-NAME/LINK-LOCAL-ADD>}
```

|                            |                                                                                |
|----------------------------|--------------------------------------------------------------------------------|
| <IP/HOSTNAME>              | Specify the remote system's IP address or hostname.                            |
| <USERNAME>                 | Specify the name of the user requesting SSH connection with the remote system. |
| <INF-NAME/ LINK-LOCAL-ADD> | Optional. Specify the interface's name or link local address.                  |

#### Example (User Exec Mode)

```

NOC-NX9500>ssh 10.234.160.13 admin
admin@10.234.160.13's password:
ap8432-070235>>ssh 192.168.13.24 admin
admin@192.168.13.24's password:
rfs4000-6DB5D4>

```

#### Example (Privi Exec Mode)

```

ap7532-DF9A4C#ssh 10.234.160.13 admin
admin@10.234.160.13's password:
ap8432-070235>

```

## telnet (user and privi exec modes)

Opens a Telnet session between two network devices



### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
telnet <IP/HOSTNAME> {<TCP-PORT>} {<INTF-NAME>}
```

### Parameters

```
telnet <IP/HOSTNAME> {<TCP-PORT>} {<INTF-NAME>}
```

|               |                                                                                                                                                                                                                                                                                                                |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IP/HOSTNAME> | Configures the destination remote system's IP (IPv4 or IPv6) address or hostname. The Telnet session is established between the connecting system and the remote system. <ul style="list-style-type: none"><li>• &lt;IP/HOSTNAME&gt; - Specify the remote system's IPv4 or IPv6 address or hostname.</li></ul> |
| <TCP-PORT>    | Optional. Specify the <i>Transmission Control Protocol</i> (TCP) port number.                                                                                                                                                                                                                                  |
| <INTF-NAME>   | Optional. Specify the interface name for the link local address.                                                                                                                                                                                                                                               |

### Examples (User Exec Mode)

```
NOC-NX9500>telnet 10.234.160.11
telnet: cannot connect to remote host (10.234.160.11): Connection refused
NOC-NX9500>telnet 10.234.160.13
```

```
Entering character mode
Escape character is '^']'.
```

```
AP8432 release 5.9.2.0-029R
ap8432-070235 login:
```

### Example (Privi Exec Mode)

```
NOC-NX9500#telnet 10.234.160.12
```

```
Entering character mode
Escape character is '^']'.
```

```
AP7532 release 5.9.2.0-029R
ap7532-DF9A4C login:
```

*terminal (user and privi exec modes)*

Sets the length and width of the CLI display window on a terminal



#### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
terminal [length|width] <0-512>
```

#### Parameters

```
terminal [length|width] <0-512>
```

|                |                                                                                                                                                                            |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| length <0-512> | Sets the number of lines displayed on a terminal window <ul style="list-style-type: none"><li>• &lt;0-512&gt; – Specify a value from 0 - 512.</li></ul>                    |
| width <0-512>  | Sets the width (the number of characters displayed) of the terminal window <ul style="list-style-type: none"><li>• &lt;0-512&gt; – Specify a value from 0 - 512.</li></ul> |

#### Example (User Exec Mode)

```
ap8432-070235>show terminal
Terminal Type: xterm
Length: 24 Width: 80
ap8432-070235>
ap8432-070235>terminal length 80
ap8432-070235>terminal width 100
ap8432-070235>show terminal
Terminal Type: xterm
Length: 80 Width: 100
ap8432-070235>
```

#### Example (Privi Exec Mode)

```
NOC-NX9500#show terminal
Terminal Type: xterm
Length: 24 Width: 80
NOC-NX9500#
NOC-NX9500#terminal length 30
NOC-NX9500#terminal width 100
NOC-NX9500#show terminal
Terminal Type: xterm
Length: 30 Width: 100
NOC-NX9500#
```

## Related Commands

`no (user exec mode)` on Resets the width or length of the terminal window  
page 83

`no (priv-exec-mode)` on Resets the width or length of the terminal window  
page 189

### *time-it (user and privi exec modes)*

Verifies the time taken by a particular command between request and response



#### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
time-it <COMMAND>
```

### Parameters

```
time-it <COMMAND>
```

`time-it <COMMAND>` Verifies the time taken by a particular command to execute and provide a result

- `<COMMAND>` – Specify the command.

### Examples

```
ap8432-070235>time-it enable
That took 0.00 seconds..
ap8432-070235#
```

#### Example (Privi Exec Mode)

```
rfs4000-229D58#time-it config terminal
Enter configuration commands, one per line. End with CNTL/Z.
That took 0.00 seconds..
rfs4000-229D58(config)#
```

### *traceroute (user-privi-exec-mode)*

Traces the route to a defined destination

Use '--help' or '-h' to display a complete list of parameters for the traceroute command



#### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
traceroute <LINE>
```

### Parameters

```
traceroute <LINE>
```

|                   |                                                                                                                    |
|-------------------|--------------------------------------------------------------------------------------------------------------------|
| traceroute <LINE> | Traces the route to a destination IP address or hostname                                                           |
|                   | <ul style="list-style-type: none"><li>• &lt;LINE&gt; - Specify the destination IPv4 address or hostname.</li></ul> |

### Example (User Exec Mode)

```
NOC-NX9500>traceroute 10.234.160.13
traceroute to 10.234.160.13 (10.234.160.13), 30 hops max, 46 byte packets
 1 10.234.160.13 (10.234.160.13) 0.315 ms 0.159 ms 0.137 ms
NOC-NX9500>
```

### Example (Privi Exec Mode)

```
NOC-NX9500#traceroute 10.234.160.11
traceroute to 10.234.160.11 (10.234.160.11), 30 hops max, 46 byte packets
 1 10.234.160.11 (10.234.160.11) 8.115 ms 0.410 ms 0.370 ms
NOC-NX9500#
```

### traceroute6 (user-privi-exec-mode)

Traces the route to a specified IPv6 destination



#### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
traceroute6 <LINE>
```

### Parameters

```
traceroute6 <LINE>
```

|                    |                                                                                                                    |
|--------------------|--------------------------------------------------------------------------------------------------------------------|
| traceroute6 <LINE> | Traces the route to a destination IPv6 address or hostname                                                         |
|                    | <ul style="list-style-type: none"><li>• &lt;LINE&gt; - Specify the destination IPv6 address or hostname.</li></ul> |

### Example (User Exec Mode)

```
rfs4000-6DB5D4>traceroute6 2001:10:10:10:10:10:10:1
traceroute to 2001:10:10:10:10:10:10:1 (2001:10:10:10:10:10:10:1) from
2001:10:10:10:10:10:10:2, 30 hops max, 16 byte packets
 1 2001:10:10:10:10:10:10:1 (2001:10:10:10:10:10:10:1) 6.054 ms 0.448 ms 0.555 ms
rfs4000-6DB5D4>
```

### Example (Priv Exec Mode)

```
rfs4000-229D587#traceroute6 2001:10:10:10:10:10:10:2
traceroute to 2001:10:10:10:10:10:10:2 (2001:10:10:10:10:10:10:2) from
2001:10:10:10:10:10:10:1, 30 hops max, 16 byte packets
 1 2001:10:10:10:10:10:10:2 (2001:10:10:10:10:10:10:2) 0.622 ms 0.497 ms 0.531 ms
rfs4000-229D58#
```

*virtual-machine* (user and privi exec modes)

Installs, configures, and monitors the status of virtual machines (VMs)



#### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

### Supported in the following platforms:

- Service Platforms — NX 95XX, NX 96XX, VX 9000

### Syntax

```
virtual-machine [assign-usb-ports|console|export|install|restart|set|start|stop|uninstall]
virtual-machine assign-usb-ports team-vowlan {on <DEVICE-NAME>}
virtual-machine export <VM-NAME> [<FILE>|<URL>] {on <DEVICE-NAME>}
virtual-machine install [<VM-NAME>|adsp|team-urc|team-rls|team-vowlan]
virtual-machine restart [<VM-NAME>|hard|adsp|team-urc|team-rls|team-vowlan]
virtual-machine set [autostart|memory|vcpus|vif-count|vif-mac|vif-to-vmif|vnc]
virtual-machine set [autostart [ignore|start]|memory <512-8192>|vcpus <1-4>|
vif-count <0-2>|vif-mac <VIF-INDEX> <MAC-INDEX>|vif-to-vmif <VIF-INDEX> <VMIF-INDEX>|
vnc [disable|enable]] [<VM-NAME>|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}
```

The following virtual-machine commands are supported only on the VX 9000 platform:

```
virtual-machine volume-group [add-drive|replace-drive|resize-drive|resize-volume-group]
virtual-machine volume-group [add-drive|replace-drive] <BLOCK-DEVICE-LABEL>
virtual-machine volume-group replace-drive <BLOCK-DEVICE-LABLE> <NEW-BLOCK-DEVICE-
LABEL>
virtual-machine volume-group resize-volume-group <BLOCK-DEVICE-LABEL>
```

### Parameters

```
virtual-machine assign-usb-ports team-vowlan {on <DEVICE-NAME>}
```

assign-usb-ports team-vowlan

Assigns USB ports to TEAM-VoWLAN on a specified device

- on <DEVICE-NAME> – Optional. Specify the device name.

**Note:** Use the **no > virtual-machine > assign-usb-ports** command to reassign the port to WiNG.

**Note:** TEAM-RLS VM cannot be installed when USB ports are assigned to TEAM-VoWLAN.

```
virtual-machine export <VM-NAME> [<FILE>|<URL>] {on <DEVICE-NAME>}
```

virtual-machine export

Exports an existing VM image and settings. Use this command to export the VM to another device in the same domain.

- <VM-NAME> – Specify the VM name.
- <FILE> – Specify the location and name of the source file (VM image). The VM image is retrieved and exported from the specified location.
- <URL> – Specify the destination location. This is the location to which the VM image is copied. Use one of the following formats to provide the destination path:
  - tftp://<hostname|IP>[:port]/path/file
  - ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file
  - sftp://<user>:<passwd>@<hostname|IP>[:port]/path/file
  - http://<hostname|IP>[:port]/path/file
- on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices
- <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.

**Note:** The VM should be in a stop state during the export process.

**Note:** If the destination is a device, the image is copied to a predefined location (VM archive).

```
virtual-machine install [<VM-NAME>|adsp|team-centro|team-rls|team-vowlan] {on <DEVICE-NAME>}
```

virtual-machine install

Installs the VM. The install command internally creates a VM template, consisting of the specified parameters, and starts the installation process.

- <VM-NAME> – Specify the VM name.
- adsp – Installs ADSP
- team-centro – Installs the VM TEAM-Centro image
- team-rls – Installs the VM TEAM-RLS image
- team-vowlan – Installs the VM TEAM-VoWLAN image

Specify the device on which to install the VM.

- on <DEVICE-NAME> – Optional. Executes the command on a specified device or devices
- <DEVICE-NAME> – Specify the service platform name. In case of multiple devices, list the device names separated by commas.

```
virtual-machine set [autostart [ignore|start]]|memory <512-8192>|vcpus <1-4>|vif-count <0-2>|vif-mac <VIF-INDEX> <MAC-INDEX>|vif-to-vmif <VIF-INDEX> <VMIF-INDEX>|vnc [disable|enable]] [<VM-NAME>|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}
```

virtual-machine  
set

Configures the VM settings

- autostart – Specifies whether to autostart the VM on system reboot
  - ignore – Enables autostart on each system reboot
  - start – Disables autostart
- memory – Defines the VM memory size
  - <512-8192> – Specify the VM memory from 512 - 8192 MB. The default is 1024 MB.
- vcpus – Specifies the number of VCPUS for this VM
  - <1-4> – Specify the number of VCPUS from 1- 4.
- vif-count – Configures or resets the VM's VIFs
  - <0-2> – Specify the VIF number from 0 - 2.
- vif-mac – Configures the MAC address of the selected virtual network interface
  - <1-2> – Select the VIF
    - <1-8> – Specify the MAC index for the selected VIF
    - <MAC> – Specify the customized MAC address for the selected VIF in the AA-BB-CC-DD-EE-FF format.

Each VM has a maximum of two network interfaces (indexed 1 and 2, referred to as VIF). By default, each VIF is automatically assigned a MAC from the range allocated for that device. However, you can use the 'set' keyword to specify the MAC from within the allocated range. Each of these VIFs are mapped to a layer 2 port in the dataplane (referred to as VMIF). These VMIFs are standard I2 ports on the DP bridge, supporting all VLAN and ACL commands. The WiNG software supports up to a maximum of 8 VMIFs. By default, a VM's interface is always mapped to VMIF1. You can map a VIF to any of the 8 VMIFs. Use the vif-to-vmif command to map a VIF to a VMIF on the DP bridge.

- vif-to-vmif – Maps the virtual interface (1 or 2) to the selected VMIF interface. Specify the VMIF interface index from 1 - 8.

WiNG provides a dataplane bridge for external network connectivity for VMs. VM Interfaces define which IP address is associated with each VLAN ID the service platform is connected to and enables remote service platform administration. Each custom VM can have up to a maximum of two VM interfaces. Each VM interface can be mapped to one of the twelve ports for NX 95XX on the dataplane bridge. This mapping determines the destination for service platform routing.

By default, VM interfaces are internally connected to the dataplane bridge via VMIF1. VMIF1, by default, is an untagged port providing access to VLAN 1 to support the capability to connect the VM interfaces to any of the VMIF ports. This provides the flexibility to move a VM interface onto different VLANs as well as configure specific firewall and QoS rules.

- vnc – Disables/enables VNC port option for an existing VM. When enabled, provides remote access to VGA through the noVNC client.
  - disable – Disables VNC port
  - enable – Enables VNC port

After configuring the VM settings, identify the VM to apply the settings.

- <VM-NAME> – Applies these settings to the VM identified by the <VM-NAME> keyword. Specify the VM name.
- adsp – Applies these settings to the ADSP VM
- team-urc – Applies these settings to the VM TEAM-URC
- team-rls – Applies these settings to the VM TEAM-RLS
- team-vowlan – Applies these settings to the VM TEAM-VoWLAN

```
virtual-machine start [<VM-NAME>|adsp|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}
```



virtual-machine start Starts the VM, based on the parameters passed. Select one of the following options:

- <VM-NAME> - Starts the VM identified by the <VM-NAME> keyword. Specify the VM name.
- adsp - Starts the ADSP VM
- team-urc - Starts the VM TEAM-URC
- team-rls - Starts the VM TEAM-RLS
- team-vowlan - Starts the VM TEAM-VoWLAN

The following keywords are common to all of the above parameters:

- on <DEVICE-NAME> - Optional. Executes the command on a specified device or devices
  - <DEVICE-NAME> - Specify the service platform name. In case of multiple devices, list the device names separated by commas.

```
virtual-machine stop [<VM-NAME>|adsp|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}
```

virtual-machine stop hard Stops the VM, based on the parameters passed. Select one of the following options:

- <VM-NAME> - Stops the VM identified by the <VM-NAME> keyword. Specify the VM name.
- ADSP - Stops the ADSP VM
- team-urc - Stops the VM TEAM-URC
- team-rls - Stops the VM TEAM-RLS team-vowlan - Stops the VM TEAM-VoWLAN

The following keywords are common to all of the above parameters:

- on <DEVICE-NAME> - Optional. Executes the command on a specified device or devices
  - <DEVICE-NAME> - Specify the service platform name. In case of multiple devices, list the device names separated by commas. Note: The option 'hard' forces the selected VM to shutdown.

**Note:** The option 'hard' forces the selected VM to shutdown.

```
virtual-machine uninstall [<VM-NAME>|adsp|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}
```

virtual-machine uninstall Uninstalls the specified VM

- <VM-NAME> - Uninstalls the VM identified by the <VM-NAME> keyword. Specify the VM name.
- ADSP - Uninstalls the ADSP VM
- team-urc - Uninstalls the VM TEAM-URC
- team-rls - Uninstalls the VM TEAM-RLS team-vowlan - Stops the VM TEAM-VoWLAN

The following keywords are common to all of the above parameters:

- on <DEVICE-NAME> - Optional. Executes the command on a specified device or devices
  - <DEVICE-NAME> - Specify the service platform name. In case of multiple devices, list the device names separated by commas.

**Note:** This command releases the VM's resources, such as memory, VCPUS, VNC port, disk space, and removes the RF Domain reference from the system.

```
virtual-machine volume-group [add-drive|resize-drive] <BLOCK-DEVICE-LABEL>
```

|                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>virtual-machine volume-group [add-drive] [resize-drive] &lt;BLOCK- DEVICE- LABEL&gt;]</pre> | <p>Enables provisioning of logical volume-groups on the VX 9000 platform. Logical volume-groups are created on the primary storage device, allowing the database storage to be expanded to include additional storage drives. However, volume-groups can be provisioned only on new VX 9000 installation and cannot be added to existing VX 9000 installation.</p> <p><b>Note:</b> The logical volume-group is supported only on a VX 9000 running the WiNG 5.9.1 and above version.</p> <ul style="list-style-type: none"> <li>• <b>add-drive</b> – Adds a new block-device to the VM. Note, currently a maximum of 3 (three) block devices can be added. To add a new drive, first halt the VM, In the Hypervisor, add a new storage disk to the VM and restart the VM. Once the VM comes up, use this command to add the new drive. To identify the new drive execute the <b>show &gt; virtual-machine &gt; volume-group &gt; status</b> command.</li> <li>• <b>resize-drive</b> - Resizes a drive in the VM's volume group. To increase the size of a drive in the volume-group, first halt the VM. In the Hypervisor, increase the size of the existing secondary storage drive and restart the VM. Once the VM comes up, use this command to resize the drive. To identify the drive with the additional free space, execute the <b>show &gt; virtual-machine &gt; volume-group &gt; status</b> command.</li> </ul> <p>The following keyword is common to all of the above parameters:</p> <ul style="list-style-type: none"> <li>• <b>&lt;BLOCK-DEVICE-LABEL&gt;</b> -Specify the block-device label to be added or resized depending on the action being performed.</li> </ul> |
|--------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
virtual-machine volume-group replace-drive <BLOCK-DEVICE-LABEL> <NEW-BLOCK-DEVICE-LABEL>
```

|                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>virtual-machine volume-group replace-drive &lt;BLOCK- DEVICE-LABEL&gt; &lt;NEW- BLOCK-DEVICE-LABEL&gt;]</pre> | <p>Enables provisioning of VMs as logical volume-groups on the VX 9000 platform. Logical volume-group VMs are created on the primary storage device, allowing the database storage to be expanded to include additional storage drives.</p> <ul style="list-style-type: none"> <li>• <b>replace-drive</b> – Replaces an existing block-device with a new block-device in a volume-group. To replace a drive in the volume-group, first halt the VM. In the Hypervisor, add the new drive and restart the VM. Once the VM comes up, use this command to replace an existing drive with the new drive. To identify the drive with the additional free space, execute the <b>show &gt; virtual-machine &gt; volume-group &gt; status</b> command <ul style="list-style-type: none"> <li>• <b>&lt;BLOCK-DEVICE-LABEL&gt;</b> -Specify the block-device label to be replaced.</li> <li>• <b>&lt;BLOCK-DEVICE-LABEL&gt;</b> - Specify the replacement block-device label.</li> </ul> </li> </ul> |
|--------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
virtual-machine volume-group resize-volume-group <BLOCK-DEVICE-LABEL>
```

|                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>virtual-machine volume- group resize-volume-group &lt;BLOCK-DEVICE-LABEL&gt;</pre> | <p>Enables provisioning of VMs as logical volume-groups on the VX 9000 platform. Logical volume-group VMs are created on the primary storage device, allowing the database storage to be expanded to include additional storage drives</p> <ul style="list-style-type: none"> <li>• <b>resize-volume-group</b> – Adds drive space to an existing block-device in the volume-group <ul style="list-style-type: none"> <li>• <b>&lt;BLOCK-DEVICE-LABEL&gt;</b> -Specify the block-device label to which additional drive space is to be provided</li> </ul> </li> </ul> |
|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

The following examples show the VM installation process:

### Insatllation media: USB

```
<DEVICE>#virtual-machine install <VM-NAME> type iso disk-size 8 install-media usb1://vms/
win7.iso autostart start memory 512 vcpus 3 vif-count 2 vnc enable
```

## Installation media: pre-installed disk image

```
<DEVICE>#virtual-machine install <VM-NAME> type disk install-media flash:/vms/
win7_disk.img autostart start memory 512 vcpus 3 vif-count 2 vnc-enable on <DEVICE-NAME>
In the preceding example, the command is executed on the device identified by the <DEVICE-
NAME> keyword. In such a scenario, the disk-size is ignored if specified. The VM has the
install media as first boot device.
```

## Installation media: VM archive

```
<DEVICE>#virtual-machine install type vm-archive install-media flash:/vms/<VM-NAME> vcpus 3
In the preceding example, the default configuration attached with the VM archive overrides
any parameters specified.
```

## Exporting an installed VM:

```
<DEVICE>#virtual-machine export <VM-NAME> <URL> on <DEVICE-NAME>
In the preceding example, the command copies the VM archive on to the URL (VM should be in
stop state).
<DEVICE>>virtual-machine install team-urc
Virtual Machine install team-urc command successfully sent.
<DEVICE>>
VX 9000-DE6F97>virtual-machine add-drive sdb
VX 9000-DE6F97>show virtual-machine volume-group status

Logical Volume: lv1

STATUS : available
SIZE : 81.89 GiB
VOLUME GROUP : vg0
PHYSICAL VOLUMES :
 sda10 : 73.90 GiB
 sdc1 : 8.00 GiB
AVAILABLE DISKS :
 sdb : size: 8590MB

* indicates a drive that must be resized

VX 9000-DE6F97>
```

*exit (user exec mode)*

Ends the current CLI session and closes the session window

For more information, see [exit](#).

## Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

`exit`

## Parameters

None

## Examples

```
nx9500-6C8809>exit
```

### *watch*

Repeats the specified CLI command at periodic intervals

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
watch <1-3600> <LINE>
```

### Parameters

```
watch <1-3600> <LINE>
```

|          |                                                                                       |
|----------|---------------------------------------------------------------------------------------|
| watch    | Repeats a CLI command at a specified interval (in seconds)                            |
| <1-3600> | Select an interval from 1 - 3600 sec. Pressing CTRL-Z halts execution of the command. |
| <LINE>   | Specify the CLI command.                                                              |

### Examples

In the following example, the controller pings the specified IP address once in every 40 seconds.

```
NOC-NX9500>watch 40 ping 10.234.160.13
PING 10.234.160.13 (10.234.160.13) 100(128) bytes of data.
108 bytes from 10.234.160.13: icmp_seq=1 ttl=64 time=0.257 ms
108 bytes from 10.234.160.13: icmp_seq=2 ttl=64 time=0.176 ms
108 bytes from 10.234.160.13: icmp_seq=3 ttl=64 time=0.170 ms
108 bytes from 10.234.160.13: icmp_seq=4 ttl=64 time=0.170 ms
108 bytes from 10.234.160.13: icmp_seq=5 ttl=64 time=0.169 ms

--- 10.234.160.13 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
rtt min/avg/max/mdev = 0.169/0.188/0.257/0.036 ms
PING 10.234.160.13 (10.234.160.13) 100(128) bytes of data.
108 bytes from 10.234.160.13: icmp_seq=1 ttl=64 time=0.251 ms
108 bytes from 10.234.160.13: icmp_seq=2 ttl=64 time=0.174 ms
108 bytes from 10.234.160.13: icmp_seq=3 ttl=64 time=0.154 ms
108 bytes from 10.234.160.13: icmp_seq=4 ttl=64 time=0.170 ms
108 bytes from 10.234.160.13: icmp_seq=5 ttl=64 time=0.169 ms

--More--
NOC-NX9500>
```

# PRIVILEGED EXEC MODE COMMANDS

## PRIVILEGED EXEC MODE COMMANDS

---

Most PRIV EXEC commands set operating parameters. Privileged-level access should be password protected to prevent unauthorized use. The PRIV EXEC command set includes commands contained within the USER EXEC mode. The PRIV EXEC mode also provides access to configuration modes, and includes advanced testing commands.



### Note

To password-protect the Privilege mode, in the Management Policy, configure the `privilege-mode-password`. For more information, see [privilege-mode-password](#) on page 1532.

---

The PRIV EXEC mode prompt consists of the hostname of the device followed by a pound sign (#).

To access the PRIV EXEC mode, enter the following at the prompt:

```
<DEVICE>>enable
<DEVICE>#
```

The PRIV EXEC mode is often referred to as the enable mode, because the enable command is used to enter the mode.

There is no provision to configure a password to get direct access to PRIV EXEC (enable) mode.

```
<DEVICE>#?
Privileged command commands:
 <DEVICE>#?
Privileged command commands:
 archive Manage archive files
 boot Boot commands
 captive-portal-page-upload Captive portal internal and advanced page upload
 cd Change current directory
 change-passwd Change password
 clear Clear
 clock Configure software system clock
 cluster Cluster commands
 commit Commit all changes made in this session
 configure Enter configuration mode
 connect Open a console connection to a remote device
 copy Copy contents of one dir to another
 cpe T5 CPE configuration
 create-cluster Create a cluster
 crypto Encryption related commands
 crypto-cmp-cert-update Update the cmp certs
 database Database
 database-backup Backup database
 database-restore Restore database
 debug Debugging functions
 delete Deletes specified file from the system
 device-upgrade Device firmware upgrade
 diff Display differences between two files
 dir List files on a filesystem
 disable Turn off privileged mode command
 edit Edit a text file
 enable Turn on privileged mode command
```

|                 |                                                                                                                    |
|-----------------|--------------------------------------------------------------------------------------------------------------------|
| erase           | Erase a filesystem                                                                                                 |
| ex3500          | EX3500 commands                                                                                                    |
| factory-reset   | Delete startup configuration on device(s), reload the device(s) and remove configuration entry from the controller |
| file-sync       | File sync between controller and adoptees                                                                          |
| format          | Format file system                                                                                                 |
| halt            | Halt the system                                                                                                    |
| help            | Description of the interactive help system                                                                         |
| join-cluster    | Join the cluster                                                                                                   |
| l2tpv3          | L2tpv3 protocol                                                                                                    |
| logging         | Modify message logging facilities                                                                                  |
| mint            | MiNT protocol                                                                                                      |
| mkdir           | Create a directory                                                                                                 |
| more            | Display the contents of a file                                                                                     |
| no              | Negate a command or set its defaults                                                                               |
| on              | On RF-Domain                                                                                                       |
| opendns         | Opendns username/password configuration                                                                            |
| page            | Toggle paging                                                                                                      |
| ping            | Send ICMP echo messages                                                                                            |
| ping6           | Send ICMPv6 echo messages                                                                                          |
| pwd             | Display current directory                                                                                          |
| raid            | RAID operations                                                                                                    |
| re-elect        | Perform re-election                                                                                                |
| reload          | Halt and perform a warm reboot                                                                                     |
| remote-debug    | Troubleshoot remote system(s)                                                                                      |
| rename          | Rename a file                                                                                                      |
| revert          | Revert changes                                                                                                     |
| rmdir           | Delete a directory                                                                                                 |
| self            | Config context of the device currently logged into                                                                 |
| service         | Service Commands                                                                                                   |
| show            | Show running system information                                                                                    |
| ssh             | Open an ssh connection                                                                                             |
| t5              | T5 commands                                                                                                        |
| telnet          | Open a telnet connection                                                                                           |
| terminal        | Set terminal line parameters                                                                                       |
| time-it         | Check how long a particular command took between request and completion of response                                |
| traceroute      | Trace route to destination                                                                                         |
| traceroute6     | Trace route to destination(IPv6)                                                                                   |
| upgrade         | Upgrade software image                                                                                             |
| upgrade-abort   | Abort an ongoing upgrade                                                                                           |
| virtual-machine | Virtual Machine                                                                                                    |
| watch           | Repeat the specific CLI command at a periodic interval                                                             |
| write           | Write running configuration to memory or terminal                                                                  |
| clrscr          | Clears the display screen                                                                                          |
| exit            | Exit from the CLI                                                                                                  |
| <DEVICE>        |                                                                                                                    |

## privileged-exec-commands

The following table summarizes the PRIV EXEC configuration mode commands:

**Table 5: Privileged Exec Commands**

| Command                                                                           | Description                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">archive</a> on page 109                                               | Manages file archive operations                                                                                                                                                                                                             |
| <a href="#">boot</a> on page 111                                                  | Specifies the boot partition as primary or secondary. The device boots using the image stored in the specified partition.                                                                                                                   |
| <a href="#">captive-portal-page-upload (user and privi exec modes)</a> on page 27 | Uploads captive portal advanced pages to adopted access points                                                                                                                                                                              |
| <a href="#">cd</a> on page 116                                                    | Changes the current directory                                                                                                                                                                                                               |
| <a href="#">change-passwd (user and privi exec modes)</a> on page 31              | Changes the password of the currently logged-in user                                                                                                                                                                                        |
| <a href="#">clear (user and privi exec modes)</a> on page 32                      | Clears parameters, cache entries, table entries, and other similar entries                                                                                                                                                                  |
| <a href="#">clock (user and privi exec modes)</a> on page 44                      | Configures the system clock                                                                                                                                                                                                                 |
| <a href="#">cluster (user and privi exec modes)</a> on page 46                    | Initiates a cluster context                                                                                                                                                                                                                 |
| <a href="#">configure</a>                                                         | Enters the global configuration mode                                                                                                                                                                                                        |
| <a href="#">connect (user and privi exec modes)</a> on page 46                    | Begins a console connection to a remote device                                                                                                                                                                                              |
| <a href="#">copy</a> on page 133                                                  | Clears parameters, cache entries, table entries, and other similar entries                                                                                                                                                                  |
| <a href="#">cpe (privilege-exec-mode)</a> on page 134                             | Enables adopted T5 CPE (Customer Premises Equipment) device(s) management. Use this command to perform the following operations on the CPEs: boot, reload, upgrade. This command is specific to the RFS 4000, NX 95XX, and NX 96XX devices. |
| <a href="#">create-cluster (user and privi exec modes)</a> on page 47             | Creates a new cluster on a specified device                                                                                                                                                                                                 |
| <a href="#">crypto (user and privi exec modes)</a> on page 49                     | Enables encryption                                                                                                                                                                                                                          |
| <a href="#">crypto-cmp-cert-policy (user and privi exec modes)</a> on page 58     | Triggers a CMP certificate update on a specified device or devices                                                                                                                                                                          |
| <a href="#">database (user and privi exec modes)</a> on page 59                   | Enables automatic repairing (vacuuming) and dropping of databases (Captive-portal and NSight)                                                                                                                                               |
| <a href="#">database-backup (user and privi exec modes)</a> on page 63            | Backs up captive-portal and/or NSight database to a specified location and file on an FTP or SFTP server                                                                                                                                    |
| <a href="#">database-backup (user and privi exec modes)</a> on page 63            | Restores a previously exported database [captive-portal and/or NSight]. Previously exported databases (backed up to a specified FTP or SFTP server) are restored to the original database.                                                  |
| <a href="#">delete</a> on page 161                                                | Deletes a specified file from the system                                                                                                                                                                                                    |
| <a href="#">device-upgrade (user and privi exec modes)</a> on page 65             | Configures device firmware upgrade parameters                                                                                                                                                                                               |
| <a href="#">diff</a> on page 162                                                  | Displays the differences between two files                                                                                                                                                                                                  |
| <a href="#">dir</a> on page 162                                                   | Displays the list of files on a file system                                                                                                                                                                                                 |

**Table 5: Privileged Exec Commands (continued)**

| Command                                                          | Description                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>disable</code> on page 164                                 | Disables the privileged mode command set                                                                                                                                                                                                                      |
| <code>edit</code> on page 164                                    | Edits a text file                                                                                                                                                                                                                                             |
| <code>enable</code> on page 165                                  | Turns on (enables) the privileged mode commands set                                                                                                                                                                                                           |
| <code>erase</code> on page 165                                   | Erases a file system                                                                                                                                                                                                                                          |
| <code>ex3500</code> on page 167                                  | Enables EX3500 switch firmware management. Use this command to perform the following operations: boot, copy, delete, and IP related configurations.                                                                                                           |
| <code>factory-reset</code> on page 175                           | Erases startup configuration on a specified device or all devices within a specified RF Domain                                                                                                                                                                |
| <code>file-sync (user and privi exec modes)</code> on page 74    | Configures parameters enabling syncing of PKCS#12 and wireless-bridge certificate between the staging-controller and adopted access points                                                                                                                    |
| <code>halt</code> on page 181                                    | Halts a device (Access Point, wireless controller, or service platform)                                                                                                                                                                                       |
| <code>join-cluster (user and privi exec modes)</code> on page 77 | Adds a device (Access Point, wireless controller, or service platform), as cluster member, to an existing cluster of devices                                                                                                                                  |
| <code>l2tpv3 (user and privi exec modes)</code> on page 79       | Establishes or brings down L2TPV3 tunnels                                                                                                                                                                                                                     |
| <code>logging (user and privi exec modes)</code> on page 80      | Modifies message logging parameters                                                                                                                                                                                                                           |
| <code>mint (user and privi exec modes)</code> on page 82         | Configures MINT protocols                                                                                                                                                                                                                                     |
| <code>mkdir</code> on page 188                                   | Creates a new directory in the file system                                                                                                                                                                                                                    |
| <code>more</code> on page 189                                    | Displays the contents of a file                                                                                                                                                                                                                               |
| <code>on (user and privi exec modes)</code> on page 84           | Reverts a command or sets values to their default                                                                                                                                                                                                             |
| <code>on (user and privi exec modes)</code> on page 84           | Executes the following commands in the RF Domain context: <code>clrscr</code> , <code>do</code> , <code>end</code> , <code>exit</code> , <code>help</code> , <code>service</code> , and <code>show</code>                                                     |
| <code>opendns (user and privi exec modes)</code> on page 86      | Connects to the OpenDNS site using OpenDNS registered credentials (username, password) OR OpenDNS API token to fetch the OpenDNS device_id. This command is a part of the process integrating access points, controllers, and service platforms with OpenDNS. |
| <code>page (user and privi exec modes)</code> on page 89         | Toggles a device's (Access Point, wireless controller, or service platform) paging function                                                                                                                                                                   |
| <code>ping (user and privi exec modes)</code> on page 90         | Sends ICMP echo messages to a user-specified location                                                                                                                                                                                                         |
| <code>ping6 (user and privi exec modes)</code> on page 91        | Sends ICMPv6 echo messages to a user-specified location                                                                                                                                                                                                       |
| <code>pwd</code> on page 199                                     | Displays the current directory                                                                                                                                                                                                                                |
| <code>re-elect</code> on page 200                                | Re-elects the tunnel controller (wireless controller, service platform, or Access Point)                                                                                                                                                                      |
| <code>reload</code> on page 200                                  | Halts a device (wireless controller, service platform, or Access Point) and performs a warm reboot                                                                                                                                                            |
| <code>rename</code> on page 205                                  | Renames a file in the existing file system                                                                                                                                                                                                                    |



**Table 5: Privileged Exec Commands (continued)**

| Command                                                                | Description                                                                                                                                   |
|------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">rmdir</a> on page 206                                      | Deletes an existing file from the file system                                                                                                 |
| <a href="#">self</a> on page 207                                       | Displays the configuration context of the device                                                                                              |
| <a href="#">ssh (user and privi exec modes)</a> on page 93             | Connects to another device using a secure shell                                                                                               |
| <a href="#">t5 (privi exec mode)</a> on page 208                       | Executes the following operations on a T5 device: copy, rename, delete, and write. This command is specific to the RFS 4000, NX 95XX devices. |
| <a href="#">telnet (user and privi exec modes)</a> on page 94          | Opens a Telnet session                                                                                                                        |
| <a href="#">terminal (user and privi exec modes)</a> on page 95        | Sets the length and width of the terminal window                                                                                              |
| <a href="#">time-it (user and privi exec modes)</a> on page 96         | Verifies the time taken by a particular command between request and response                                                                  |
| <a href="#">traceroute (user-privi-exec-mode)</a> on page 96           | Traces the route to a defined IPv4 destination                                                                                                |
| <a href="#">traceroute6 (user-privi-exec-mode)</a> on page 97          | Traces the route to a defined IPv6 destination                                                                                                |
| <a href="#">upgrade</a> on page 214                                    | Upgrades the software image                                                                                                                   |
| <a href="#">upgrade-abort</a> on page 218                              | Aborts an ongoing software image upgrade                                                                                                      |
| <a href="#">exit (privi exec mode)</a> on page 167                     | Ends the current CLI session and closes the session window                                                                                    |
| <a href="#">watch</a> on page 226                                      | Repeats the specific CLI command at a periodic interval                                                                                       |
| <a href="#">virtual-machine (user and privi exec modes)</a> on page 98 | Installs, configures, and monitors the status of VMs. This command is specific to the NX 9500 and NX 9510 series service platforms.           |
| <a href="#">raid</a> on page 225                                       | Enables RAID management. This command is specific to the NX 9500 series service platforms.                                                    |

**Note**

For information on common commands (clscr, commit, help, revert, service, show, write, and exit), see [COMMON COMMANDS](#) on page 640.

**Note**

The input parameter <HOSTNAME>, if used in syntaxes across this chapter, cannot include an underscore ( \_ ) character.

*archive*

Manages file archive operations

**Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000

- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
archive tar /table [<FILE>|<URL>]
archive tar /create [<FILE>|<URL>] <FILE>
archive tar /xtract [<FILE>|<URL>] <DIR>
```

### Parameters

```
archive tar /table [<FILE>|<URL>]
```

|        |                                                      |
|--------|------------------------------------------------------|
| tar    | Manipulates (creates, lists, or extracts) a tar file |
| /table | Lists the files in a tar file                        |
| <FILE> | Defines a tar filename                               |
| <URL>  | Sets the tar file URL                                |

```
archive tar /create [<FILE>|<URL>] <FILE>
```

|         |                                                     |
|---------|-----------------------------------------------------|
| tar     | Manipulates (creates, lists or extracts) a tar file |
| /create | Creates a tar file                                  |
| <FILE>  | Defines tar filename                                |
| <URL>   | Sets the tar file URL                               |

```
archive tar /xtract [<FILE>|<URL>] <DIR>
```

|         |                                                                                                                                                                                                   |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| tar     | Manipulates (creates, lists or extracts) a tar file                                                                                                                                               |
| /xtract | Extracts content from a tar file                                                                                                                                                                  |
| <FILE>  | Defines tar filename                                                                                                                                                                              |
| <URL>   | Sets the tar file URL                                                                                                                                                                             |
| <DIR>   | Specify a directory name. When used with /create, dir is the source directory for the tar file. When used with /xtract, dir is the destination file where contents of the tar file are extracted. |

### Examples

Following examples show how to zip the folder flash:/log/?

```
nx9500-6C8809#dir flash:/
```

```
Directory of flash:/
```

```
-rw- 62937 Tue Nov 24 16:00:06 2015 run-config-backup.txt
drwx Mon Apr 3 12:40:23 2017 crashinfo
drwx Wed Mar 22 13:58:28 2017 upgrade
drwx Mon Sep 28 09:48:33 2015 tmptpd
drwx Wed Apr 5 11:20:11 2017 log
drwx Thu Mar 30 15:07:54 2017 archived_logs
drwx Tue May 24 22:23:54 2016 cache
drwx Thu Feb 19 08:53:45 2015 floorplans
-rw- 42018304 Tue Sep 27 10:19:24 2016 in.tar
drwx Tue Jan 17 10:02:01 2017 hotspot
```

```
nx9500-6C8809#
```

```
nx9500-6C8809#archive tar /create flash:/in.tar flash:/log/
```

```
log/nsightd.log.1
```

```
log/nsight_reportd.log
```

```

log/messages.1.log
log/martdb.log
log/reportd.log.2
log/adopts.log.2
log/mongod.log.2
log/dpd2.log
log/nsight_server.log
log/mart_websock_server.log
log/nuxi/
log/nuxi/beanyaml.log
log/nuxi/statsreqresp.1.log
log/nuxi/hadoop.log.2014-08-03
log/nuxi/puts.log
log/nuxi/copy2w.log
log/nuxi/obj2yaml.log
log/nuxi/infl.log
--More--
nx9500-6C8809#
nx9500-6C8809#dir flash:/
Directory of flash:/

-rw- 62937 Tue Nov 24 16:00:06 2015 run-config-backup.txt
drwx Thu Sep 22 00:12:07 2016 crashinfo
drwx Sat Sep 17 05:14:43 2016 upgrade
drwx Mon Sep 28 09:48:33 2015 tmptpd
drwx Tue Sep 27 09:59:12 2016 log
drwx Mon Sep 26 09:58:54 2016 archived_logs
drwx Tue May 24 22:23:54 2016 cache
drwx Thu Feb 19 08:53:45 2015 floorplans
-rw- 42018304 Tue Sep 27 10:19:24 2016 in.tar
drwx Mon Sep 15 03:40:02 2014 hotspot

nx9500-6C8809#

```

## *boot*

Boots up a specified device or the logged device. The WiNG devices have two partitions: primary and secondary. Each of these partition contains an image of the operating system. Whenever the device boots up, it loads the image from the partition specified here.

### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### **Syntax**

```
boot system [primary|secondary] {on <DEVICE-NAME>}
```

### **Parameters**

```
boot system [primary|secondary] {on <DEVICE-NAME>}
```

|                            |                                                                                                                                                                                                                                                             |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| system [primary secondary] | Specifies the image used to boot up <ul style="list-style-type: none"> <li>primary – Uses the primary image to boot</li> <li>secondary – Uses the secondary image to boot</li> </ul>                                                                        |
| on <DEVICE-NAME>           | Optional. Boots a specified device <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul> <p><b>Note:</b> If no device is specified, the logged device boots up.</p> |

### Examples

```
nx9500-6C8809#show boot
```

| IMAGE     | BUILD DATE          | INSTALL DATE        | VERSION      |
|-----------|---------------------|---------------------|--------------|
| Primary   | 01/26/2018 01:48:56 | 01/30/2018 15:02:18 | 5.9.2.0-012D |
| Secondary | 01/15/2018 13:13:38 | 01/17/2018 13:36:50 | 5.9.2.0-010D |

```
Current Boot : Primary
Next Boot : Primary
Software Fallback : Enabled
VM support : Not present
nx9500-6C8809#
nx9500-6C8809#boot system secondary
Updated system boot partition
nx9500-6C8809#
nx9500-6C8809#show boot
```

| IMAGE     | BUILD DATE          | INSTALL DATE        | VERSION      |
|-----------|---------------------|---------------------|--------------|
| Primary   | 01/26/2018 01:48:56 | 01/30/2018 15:02:18 | 5.9.2.0-012D |
| Secondary | 01/15/2018 13:13:38 | 01/17/2018 13:36:50 | 5.9.2.0-010D |

```
Current Boot : Primary
Next Boot : Secondary
Software Fallback : Enabled
VM support : Not present
nx9500-6C8809#
```

### *captive-portal-page-upload (user and privi exec modes)*

Uploads captive portal advanced pages to adopted access points. Use this command to provide access points with specific captive portal configurations, so that they can successfully provision login, welcome, and condition pages to clients attempting to access the wireless network using the captive portal.



#### Note

Ensure that the captive portal pages to upload are \*.tar files.



#### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

## Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
captive-portal-page-upload [<CAPTIVE-PORTAL-NAME>|cancel-upload|delete-file|load-file]
captive-portal-page-upload <CAPTIVE-PORTAL-NAME> [<MAC/HOSTNAME>|all|rf-domain]
captive-portal-page-upload <CAPTIVE-PORTAL-NAME> [<MAC/HOSTNAME>|all] {upload-time <TIME>}
captive-portal-page-upload <CAPTIVE-PORTAL-NAME> rf-domain [<DOMAIN-NAME>|all]
{from-controller} {(upload-time <TIME>)}
captive-portal-page-upload cancel-upload [<MAC/HOSTNAME>|all|on rf-domain [<DOMAIN-NAME>|
all]]
captive-portal-page-upload delete-file <CAPTIVE-PORTAL-NAME> <FILE-NAME>
captive-portal-page-upload load-file <CAPTIVE-PORTAL-NAME> <URL>
```

## Parameters

```
captive-portal-page-upload <CAPTIVE-PORTAL-NAME> [<MAC/HOSTNAME>|all] {upload-time <TIME>}
```

|                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| captive-portal-page-upload <i>&lt;CAPTIVE-PORTAL-NAME&gt;</i> | Uploads advanced pages of the captive portal identified by the <i>&lt;CAPTIVE-PORTAL-NAME&gt;</i> parameter <ul style="list-style-type: none"><li>• <i>&lt;CAPTIVE-PORTAL-NAME&gt;</i> – Specify captive portal's name (should be existing and configured).</li></ul>                                                                                                                                                                                                                                                      |
| <i>&lt;MAC/HOSTNAME&gt;</i>                                   | Uploads to a specified AP <ul style="list-style-type: none"><li>• <i>&lt;MAC/HOSTNAME&gt;</i> – Specify the AP's MAC address or hostname.</li></ul>                                                                                                                                                                                                                                                                                                                                                                        |
| all                                                           | Uploads to all APs                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| upload-time <i>&lt;TIME&gt;</i>                               | Schedules an AP upload time <ul style="list-style-type: none"><li>• <i>&lt;TIME&gt;</i> – Specify upload time in the MM/DD/YYYY-HH:MM or HH:MM format.</li></ul> The scheduled upload time is your local system's time. It is not the access point, controller, service platform, or virtual controller time and it is not synced with the device.<br>To view a list of uploaded captive portal files, execute the <b>show &gt; captive-portal-page-upload &gt; list-files <i>&lt;CAPTIVE-PORTAL-NAME&gt;</i></b> command. |

```
captive-portal-page-upload <CAPTIVE-PORTAL-NAME> rf-domain [<DOMAIN-NAME>|all]
{from-controller} {(upload-time <TIME>)}
```

|                                                               |                                                                                                                                                                                                                                                                                |
|---------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| captive-portal-page-upload <i>&lt;CAPTIVE-PORTAL-NAME&gt;</i> | Uploads advanced pages of the captive portal identified by the <i>&lt;CAPTIVE-PORTAL-NAME&gt;</i> parameter <ul style="list-style-type: none"><li>• <i>&lt;CAPTIVE-PORTAL-NAME&gt;</i> – Specify the captive portal's name (should be existing and configured).</li></ul>      |
| rf-domain [ <i>&lt;DOMAIN-NAME&gt;</i>  all]                  | Uploads to all APs within a specified RF Domain or all RF Domains <ul style="list-style-type: none"><li>• <i>&lt;DOMAIN-NAME&gt;</i> – Uploads to APs within a specified RF Domain. Specify the RF Domain name.</li><li>• all – Uploads to APs across all RF Domains</li></ul> |

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| from-controller    | Optional. Uploads captive-portal pages to APs via the controller to which the APs are adopted                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| upload-time <TIME> | <p>Schedules an AP upload time</p> <ul style="list-style-type: none"> <li>• &lt;TIME&gt; – Specify upload time in the MM/DD/YYYY-HH:MM or HH:MM format.</li> </ul> <p>The scheduled upload time is your local system's time. It is not the access point, controller, service platform, or virtual controller time and it is not synched with the device.</p> <p>To view a list of uploaded captive portal files, execute the <b>show &gt; captive-portal-page-upload &gt; list-files &lt;CAPTIVE-PORTAL-NAME&gt;</b> command.</p> |

```
captive-portal-page-upload cancel-upload [<MAC/HOSTNAME>|all|on rf-domain [<DOMAIN-NAME>|all]]
```

|                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| captive-portal-page-upload cancel-upload                            | <p>Cancel a scheduled AP upload</p> <p>cancel-upload</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| cancel-upload [<MAC/HOSTNAME> all on rf-domain [<DOMAIN-NAME> all]] | <p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• &lt;MAC/HOSTNAME&gt; – Cancels scheduled upload to a specified AP. Specify the AP's MAC address or hostname.</li> <li>• all – Cancels all scheduled AP uploads</li> <li>• on rf-domain – Cancels all scheduled uploads within a specified RF Domain or all RF Domains <ul style="list-style-type: none"> <li>• &lt;DOMAIN-NAME&gt; – Cancels scheduled uploads within a specified RF Domain. Specify the RF Domain name.</li> <li>• all – Cancels scheduled uploads across all RF Domains</li> </ul> </li> </ul> |

```
captive-portal-page-upload delete-file <CAPTIVE-PORTAL-NAME> <FILE-NAME>
```

|                                        |                                                                                                                                                                                                                                                                                              |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| captive-portal-page-upload delete-file | Deletes a specified captive portal's uploaded captive-portal Web page files                                                                                                                                                                                                                  |
| <CAPTIVE-PORTAL-NAME> <FILE-NAME>      | <p>Identifies the captive-portal and Web pages to delete</p> <ul style="list-style-type: none"> <li>• &lt;CAPTIVE-PORTAL-NAME&gt; – Specify the captive portal name.</li> <li>• &lt;FILE-NAME&gt; – Specify the file name. The specified internal captive portal page is deleted.</li> </ul> |

```
captive-portal-page-upload load-file <CAPTIVE-PORTAL-NAME> <URL>
```

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| captive-portal-page-upload<br>load-file | Loads captive-portal advanced pages                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <CAPTIVE-PORTAL-NAME> <URL>             | <p>Specify the captive portal's name and location. The captive portal should be existing and configured.</p> <p>IPv4 URLs:</p> <ul style="list-style-type: none"> <li>• tftp://&lt;hostname IP&gt;[:port]/path/file</li> <li>• ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IP&gt;[:port]/path/file</li> <li>• sftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IP&gt;[:port]/path/file</li> <li>• http://&lt;hostname IP&gt;[:port]/path/file</li> <li>• cf:/path/file</li> <li>• usb&lt;n&gt;:/path/file</li> </ul> <p>IPv6 URLs:</p> <ul style="list-style-type: none"> <li>• tftp://&lt;hostname IPv6&gt;[:port]/path/file</li> <li>• ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IPv6&gt;[:port]/path/file</li> <li>• sftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IPv6&gt;[:port]/path/file</li> <li>• http://&lt;hostname IPv6&gt;[:port]/path/file</li> </ul> <p><b>Note:</b> The captive portal pages are downloaded to the controller from the location specified here. After downloading use the <b>captive-portal-page-upload &gt; &lt;CAPTIVE-PORTAL-NAME&gt; &gt; &lt;DEVICE-OR-DOMAIN-NAME&gt;</b> command to upload these pages to APs.</p> |

### Examples (User Executable Mode)

```
ap6562-B1A214>captive-portal-page-upload load-file captive_portal_test tftp://89.89.89.17/
pages_new_only.tar
ap6562-B1A214>
ap6562-B1A214>show captive-portal-page-upload load-image-status
Download of captive_portal_test advanced page file is complete
ap6562-B1A214>
ap6562-B1A214>captive-portal-page-upload captive_portal_test all

CONTROLLER STATUS MESSAGE

FC-0A-81-B1-A2-14 Success Added 6 APs to upload queue

ap6562-B1A214>
ap6562-B1A214>show captive-portal-page-upload status
Number of APs currently being uploaded : 1
Number of APs waiting in queue to be uploaded : 0

AP STATE UPLOAD TIME PROGRESS RETRIES LAST UPLOAD ERROR UPLOADED BY

ap6562-B1A738 downloading immediate 100 0 - None

ap6562-B1A214>
```

### Examples (Privilege Executable Mode)

```
ap6562-B1A214# captive-portal-page-upload load-file captive_portal_test tftp://89.89.89.17/
pages_new_only.tar
ap6562-B1A214#
ap6562-B1A214# show captive-portal-page-upload load-image-status
Download of captive_portal_test advanced page file is complete
ap6562-B1A214#
ap6562-B1A214# captive-portal-page-upload captive_portal_test all

CONTROLLER STATUS MESSAGE

```

```

FC-0A-81-B1-A2-14 Success Added 6 APs to upload queue

ap6562-B1A214#
ap6562-B1A214@show captive-portal-page-upload status
Number of APs currently being uploaded : 1
Number of APs waiting in queue to be uploaded : 0

 AP STATE UPLOAD TIME PROGRESS RETRIES LAST UPLOAD ERROR UPLOADED BY

ap6562-B1A738 downloading immediate 100 0 - None

ap6562-B1A214#

```

The following example lists captive portal CP-BW uploaded files:

```

nx7500-7F2C13@show captive-portal-page-upload list-files CP-BW

 NAME SIZE LAST MODIFIED

CP-BW-1.tar.gz 6133 2017-05-16 10:38:40
CP-BW.tar.gz 3370 2017-05-16 10:45:44

nx7500-7F2C13#

```

*cd*

Changes the current directory

**Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

**Syntax**

```
cd {<DIR>}
```

**Parameters**

```
cd {<DIR>}
```

<DIR> Optional. Changes the current directory to the directory identified by the <DIR> keyword. If a directory name is not provided, the system displays the current directory.

**Examples**

```

rfs4000-229D58#cd flash:/log/
rfs4000-229D58#pwd
flash:/log/
rfs4000-229D58#

```





## *change-passwd* (user and privi exec modes)

Changes the password of a logged user. When this command is executed without any parameters, the password can be changed interactively.



### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
change-passwd {<OLD-PASSWORD>} <NEW-PASSWORD>
```

### Parameters

```
change passwd {<OLD-PASSWORD>} <NEW-PASSWORD>
```

<OLD-PASSWORD> Optional. Specify the existing password.

<NEW-PASSWORD> Specify the new password.

**Note:** The password can also be changed interactively. To do so, press **[Enter]** after the command.

### Usage Guidelines

A password must be from 1 - 64 characters.

### Examples (User Executable Mode)

```
rfs4000-6DB5D4>change-passwd
Enter old password:
Enter new password:
Password for user 'admin' changed successfully
Please write this password change to memory(write memory) to be persistent.
rfs4000-6DB5D4#write memory
OK
rfs4000-6DB5D4>
```

### Examples (Privilege Executable Mode)

```
nx9500-6C8809#change-passwd
Enter old password:
Enter new password:
Password for user 'admin' changed successfully
Please write this password change to memory(write memory) to be persistent.
nx9500-6C8809#write memory
OK
nx9500-6C8809#
```

*clear* (user and privi exec modes)

Clears parameters, cache entries, table entries, and other similar entries. The clear command is available for specific commands only. The information cleared, using this command, depends on the mode in which the clear command is executed.



#### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
clear [arp-cache|bonjour|cdp|counters|crypto|eguest|event-history|gre|ip|ipv6|lacp|lldp|
mac-address-table|mint|role|rtls|spanning-tree|traffic-shape|vrrp]
clear arp-cache {on <DEVICE-NAME>}
clear bonjour cache {on <DEVICE-NAME>}
clear [cdp|lldp] neighbors {on <DEVICE-NAME>}
clear counters [ap|radio|wireless-client]
clear counters [ap {<MAC>}|radio {<MAC/DEVICE-NAME>} {<1-3>}|wireless-client {<MAC>}] {(on
<DEVICE-OR-DOMAIN-NAME>)}
clear crypto [ike|ipsec] sa
clear crypto ike sa [<IP>|all] {on <DEVICE-NAME>}
clear crypto ipsec sa {on <DEVICE-NAME>}
clear event-history
clear gre stats {on <DEVICE-NAME>}
clear ip [bgp|dhcp|ospf]
clear ip [bgp|dhcp|ospf]
clear ip bgp [<IP>|all|external|process]
clear ip bgp [<IP>|all|external] {in/on/out/soft}
clear ip bgp [<IP>|all|external] {in prefix-filter} {on <DEVICE-NAME>}
clear ip bgp [<IP>|all|external] {out} {(on <DEVICE-NAME>)}
clear ip bgp [<IP>|all|external] {soft {in/out}} {on <DEVICE-NAME>}
clear ip bgp process {on <DEVICE-NAME>}
clear ip dhcp bindings [<IP>|all] {on <DEVICE-NAME>}
clear ip ospf process {on <DEVICE-NAME>}
clear mac-address-table {address/interface/vlan} {on <DEVICE-NAME>}
clear ipv6 neighbor-cache {on <DEVICE-NAME>}
clear lacp [<1-4> counters|counters]
clear mac-address-table {address <MAC>/vlan <1-4094>} {on <DEVICE-NAME>}
clear mac-address-table {address/interface/mac-auth-state/vlan} {on <DEVICE-NAME>}
clear mac-address-table {address <MAC>/vlan <1-4094>} {on <DEVICE-NAME>}
clear mac-address-table {interface [<IN-NAME>/ge <1-2>/port-channel <1-2>| vmif <1-8>]}
{on <DEVICE-NAME>}
clear mac-address-table mac-auth-state address <MAC> vlan <1-4094> {on <DEVICE-NAME>}
clear mint mlcp history {on <DEVICE-NAME>}
clear role ldap-stats {on <DEVICE-NAME>}
clear rtls [aeroscout|ekahau]
clear rtls [aeroscout|ekahau] {<MAC/DEVICE-NAME> {on <DEVICE-OR-DOMAIN-NAME>}/on <DEVICE-
OR-DOMAIN-NAME>}
clear spanning-tree detected-protocols{interface/on}
clear spanning-tree detected-protocols {on <DEVICE-NAME>}
clear spanning-tree detected-protocols {interface [<INTERFACE-NAME>/ge <1-X>/me1/port-
channel <1-X>/pppoe1/up1/vlan <1-4094>/wwan1]} {on <DEVICE-NAME>}
```

```
clear traffic-shape statistics class <1-4> {(on <DEVICE-NAME>)}
clear vrrp [error-stats|stats] {on <DEVICE-NAME>}
```

### Parameters

```
clear arp-cache {on <DEVICE-NAME>}
```

|                  |                                                                                                                                                                                                        |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| arp-cache        | Clears ARP (Address Resolution Protocol) cache entries on a AP, wireless controller, or service platform. This protocol matches the layer 3 IP addresses to the layer 2 MAC addresses.                 |
| on <DEVICE-NAME> | Optional. Clears ARP cache entries on a specified device <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
clear bonjour cache {on <DEVICE-NAME>}
```

|                  |                                                                                                                                                                                                                    |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| bonjour cache    | Clears all Bonjour cached statistics. Once cleared the system has to re-discover available Bonjour services.                                                                                                       |
| on <DEVICE-NAME> | Optional. Clears all Bonjour cached statistics on a specified device <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
clear [cdp|lldp] neighbors {on <DEVICE-NAME>}
```

|                  |                                                                                                                                                                                                                         |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cdp              | Clears CDP (Cisco Discovery Protocol) (CDP) table entries                                                                                                                                                               |
| lldp             | Clears LLDP (Link Layer Discovery Protocol ) table entries                                                                                                                                                              |
| neighbors        | Clears CDP or LLDP neighbor table entries based on the option selected in the preceding step                                                                                                                            |
| on <DEVICE-NAME> | Optional. Clears CDP or LLDP neighbor table entries on a specified device <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
clear counters [ap {<MAC>}|radio {<MAC/DEVICE-NAME>} {<1-X>}|wireless-client {<MAC>}] {(on <DEVICE-OR-DOMAIN-NAME>)}
```

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| counters                      | Clears counters based on the parameters passed. The options are: AP, radio, and wireless clients.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| ap <MAC>                      | Clears counters for all APs or a specified AP <ul style="list-style-type: none"> <li>&lt;MAC&gt; - Optional. Specify the AP's MAC address.</li> </ul> <p><b>Note:</b> If no MAC address is specified, all AP counters are cleared.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| radio <MAC/DEVICE-NAME> <1-X> | Clears radio interface counters on a specified device or on all devices <ul style="list-style-type: none"> <li>&lt;MAC/DEVICE-NAME&gt; - Optional. Specify the device's hostname or MAC address. Optionally, append the radio interface number (to the radio ID) using one of the following formats: AA-BB-CC-DD-EE-FF:RX or HOSTNAME:RX (where RX is the interface number).</li> <li>&lt;1-X&gt; - Optional. Identifies the radio interface by its index. Specify the radio interface index, if not specified as part of the radio ID. Note, the number of radio interfaces available varies with the access point type.</li> </ul> <p><b>Note:</b> If no device name or MAC address is specified, all radio interface counters are cleared.</p> |

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless-client<br><MAC>   | <p>Clears counters for all wireless clients or a specified wireless client</p> <ul style="list-style-type: none"> <li>• &lt;MAC&gt; – Optional. Specify the wireless client's MAC address.</li> </ul> <p><b>Note:</b> If no MAC address is specified, all wireless client counters are cleared.</p>                                                                                                                    |
| on <DEVICE-OR-DOMAIN-NAME> | <p>The following option is common to all of the above keywords:</p> <ul style="list-style-type: none"> <li>• on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Clears AP, radio, or wireless client counters on a specified AP, wireless controller, service platform, or RF Domain.</li> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> |

```
clear crypto ike sa [<IP>|all] {on <DEVICE-NAME>}
```

|                   |                                                                                                                                                                                                                                                                     |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| crypto            | Clears encryption module's cached statistics                                                                                                                                                                                                                        |
| ike sa [<IP> all] | <p>Clears IKE (Internet Key Exchange) SAs (security associations)</p> <ul style="list-style-type: none"> <li>• &lt;IP&gt; – Clears IKE SA entries for the peer identified by the &lt;IP&gt; keyword</li> <li>• all – Clears IKE SA entries for all peers</li> </ul> |
| on <DEVICE-NAME>  | <p>Optional. Clears IKE SA entries, for a specified peer or all peers, on a specified device</p> <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul>                    |

```
clear crypto ipsec sa {on <DEVICE-NAME>}
```

|                             |                                                                                                                                                                                                                                                                                                          |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| crypto                      | Clears encryption module's cached statistics                                                                                                                                                                                                                                                             |
| ipsec sa {on <DEVICE-NAME>} | <p>Clears IPsec(Internet Protocol Security) database SAs</p> <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; – Optional. Clears IPsec SA entries on a specified device</li> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
clear eguest registration statistics
```

|                                |                                                                                                                                                                                                                                                                                                  |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| eguest registration statistics | <p>Clears EGuest registration server counters. When cleared EGuest registration details are deleted, and the show &gt; eguest &gt; registration &gt; statistics command output is null.</p> <p>This command is applicable only on the NX 95XX, NX 96XX, and VX 9000 model service platforms.</p> |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
clear gre stats {on <DEVICE-NAME>}
```

|                  |                                                                                                                                                                                                                     |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| gre stats        | Clears GRE tunnel statistics                                                                                                                                                                                        |
| on <DEVICE-NAME> | <p>Optional. Clears GRE tunnel statistics on a specified device</p> <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
clear event-history
```

|               |                                    |
|---------------|------------------------------------|
| event-history | Clears event history cache entries |
|---------------|------------------------------------|

```
clear ip bgp [<IP>|all|external] {in prefix-filter} {on <DEVICE-NAME>}
```

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip bgp [<IP> all external] | <p>Clears on-going BGP sessions based on the option selected</p> <ul style="list-style-type: none"> <li>• &lt;IP&gt; – Clears BGP session with the peer identified by the &lt;IP&gt; keyword. Specify the BGP peer's IP address.</li> <li>• all – Clears all BGP peer sessions</li> <li>• external – Clears eBGP (external BGP) peer sessions</li> </ul> <p>This command is applicable only to the RFS 4000, NX 95XX, NX 96XX, and VX 9000 platforms.</p> <p>Modifications made to BGP settings (BGP access lists, weight, distance, route-maps, versions, routing policy, etc.) take effect only after on-going BGP sessions are cleared. The <b>clear &gt; ip &gt; bgp command</b> clears BGP sessions. To reduce lose of route updates during the process, use the 'soft' option. Soft reconfiguration stores inbound/outbound route updates to be processed later and updated to the routing table. This requires high memory usage.</p> |
| in prefix-filter           | <p>Optional. Clears inbound route updates</p> <ul style="list-style-type: none"> <li>• prefix-filter – Optional. Clears the existing ORF (Outbound Route Filtering) prefix-list</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| on <DEVICE-NAME>           | <p>Optional. Clears route updates on a specified device</p> <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP or service platform.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

```
clear ip bgp [<IP>|all|external] {out} {(on <DEVICE-NAME>)}
```

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip bgp [<IP> all external] | <p>Clears on-going BGP sessions based on the option selected</p> <ul style="list-style-type: none"> <li>• &lt;IP&gt; – Clears BGP session with the peer identified by the &lt;IP&gt; keyword. Specify the BGP peer's IP address.</li> <li>• all – Clears all BGP peer sessions</li> <li>• external – Clears eBGP peer sessions</li> </ul> <p>This command is applicable only to the RFS 4000, NX 95XX, NX 96XX, and VX 9000 platforms.</p> |
| out                        | <p>Optional. Clears outbound route updates. Optionally specify the device on which to execute this command.</p>                                                                                                                                                                                                                                                                                                                            |
| on <DEVICE-NAME>           | <p>The following keyword is recursive and optional.</p> <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; – Optional. Clears BGP sessions on a specified device <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP or service platform.</li> </ul> </li> </ul>                                                                                                                        |

```
clear ip bgp [<IP>|all|external] {soft {in/out}} {on <DEVICE-NAME>}
```

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip bgp [<IP> all external] | <p>Clears on-going BGP sessions based on the option selected</p> <ul style="list-style-type: none"> <li>• &lt;IP&gt; – Clears BGP session with the peer identified by the &lt;IP&gt; keyword. Specify the BGP peer’s IP address.</li> <li>• all – Clears all BGP peer sessions</li> <li>• external – Clears external BGP (eBGP) peer sessions</li> </ul> <p>This command is applicable only to the RFS 4000, NX 95XX, NX 96XX, and VX 9000 platforms.</p>                                                                                                                                                                                                                                                                                                                                   |
| soft {in out}              | <p>Optional. Initiates soft-reconfiguration of route updates for the specified IP address</p> <ul style="list-style-type: none"> <li>• in – Optional. Enables soft reconfiguration of inbound route updates</li> <li>• out – Optional. Enables soft reconfiguration of outbound route updates</li> </ul> <p>Modifications made to BGP settings (BGP access lists, weight, distance, route-maps, versions, routing policy, etc.) take effect only after on-going BGP sessions are cleared. The <b>clear &gt; ip &gt; bgp</b> command clears BGP sessions. To reduce loss of route updates during the process, use the ‘soft’ option. Soft reconfiguration stores inbound/outbound route updates to be processed later and updated to the routing table. This requires high memory usage.</p> |
| on <DEVICE-NAME>           | <p>Optional. Initiates soft reconfiguration inbound/outbound route updates on a specified device</p> <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP or service platform.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

```
clear ip bgp process {on <DEVICE-NAME>}
```

|                  |                                                                                                                                                                                           |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip bgp process   | <p>Clears all BGP processes running</p> <p>This command is applicable only to the RFS 4000, NX 95XX, NX 96XX, and VX 9000 platforms.</p>                                                  |
| on <DEVICE-NAME> | <p>Optional. Clears all BGP processes on a specified device</p> <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP or service platform.</li> </ul> |

```
clear ip dhcp bindings [<IP>|all] {on <DEVICE-NAME>}
```

|                  |                                                                                                                                                                                                                                                   |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip               | Clears a DHCP (Dynamic Host Configuration Protocol) server’s IP address binding entries                                                                                                                                                           |
| dhcp bindings    | Clears DHCP connections and server bindings                                                                                                                                                                                                       |
| <IP>             | Clears specific address binding entries. Specify the IP address to clear binding entries.                                                                                                                                                         |
| all              | Clears all address binding entries                                                                                                                                                                                                                |
| on <DEVICE-NAME> | <p>Optional. Clears a specified address binding or all address bindings on a specified device</p> <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
clear ip ospf process {on <DEVICE-NAME>}
```

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip ospf process  | Clears already enabled <i>Open Shortest Path First</i> (OSPF) process and restarts the process                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| on <DEVICE-NAME> | Optional. Clears OSPF process on a specified device<br>OSPF is a link-state IGP (interior gateway protocol). OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighboring routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer, which makes routing decisions based solely on the destination IP address found in IP packets. <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
clear ipv6 neighbor-cache {on <DEVICE-NAME>}
```

|                           |                                                                                                                                                                                                                    |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| clear ipv6 neighbor-cache | Clears IPv6 neighbor cache entries                                                                                                                                                                                 |
| on <DEVICE-NAME>          | Optional. Clears IPv6 neighbor cache entries on a specified device <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
clear lacp [<1-4> counters|counters]
```

|                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| clear lacp [<1-4> counters counters] | Clears LACP (Link Aggregation Control Protocol) counters for a specified port-channel group or all port-channel groups configured <ul style="list-style-type: none"> <li>• &lt;1-4&gt; counters – Clears LACP counters for a specified port-channel. Specify the port-channel index number from 1 - 4. Note, LACP is supported only on the NX 5500, NX 75XX, and NX 95XX model service platforms. However, the NX 95XX series service platforms support only two (2) port-channels, and the other model service platforms support four (4) port-channels.</li> <li>• counters – Clears LACP counters for all configured port-channels on the device</li> </ul> |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
clear mac-address-table{address <MAC>/vlan <1-4094>} {on <DEVICE-NAME>}
```

|                   |                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mac-address-table | Clears MAC address forwarding table data based on the parameters passed<br>Use this command to clear the following: all or specified MAC addresses from the system, all MAC addresses on a specified interface, all MAC addresses on a specified VLAN, or the authentication state of a MAC address.                                                                                           |
| address <MAC>     | Optional. Clears a specified MAC address from the MAC address table. <ul style="list-style-type: none"> <li>• &lt;MAC&gt; – Specify the MAC address in one of the following formats: AA-BB-CC-DD-EE-FF or AA:BB:CC:DD:EE:FF or AABB.CCDD.EEFF</li> </ul> <p><b>Note:</b> If executed without specifying any MAC address(es), all MAC addresses from the MAC address table will be removed.</p> |

|                  |                                                                                                                                                                                                                                                      |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vlan <1-4094>    | Optional. Clears all MAC addresses for a specified VLAN <ul style="list-style-type: none"> <li>• &lt;1-4094&gt; – Specify the VLAN ID from 1 - 4094</li> </ul>                                                                                       |
| on <DEVICE-NAME> | Optional. Clears a single MAC entry or all MAC entries, for the specified VLAN on a specified device <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
clear mac-address-table {interface [<IF-NAME>/ge <1-X>/port-channel <1-X>]} {on <DEVICE-NAME>}
```

|                    |                                                                                                                                                                                                                                                                                                            |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mac-address-table  | Clears MAC address forwarding table data based on the parameters passed<br>Use this command to clear the following: all or specified MAC addresses from the system, all MAC addresses on a specified interface, all MAC addresses on a specified VLAN, or the authentication state of a MAC address.       |
| interface          | Clears all MAC addresses for the selected interface. Use the options available to specify the interface.                                                                                                                                                                                                   |
| <IF-NAME>          | Clears MAC address forwarding table for the specified layer 2 interface (Ethernet port) <ul style="list-style-type: none"> <li>• &lt;IF-NAME&gt; – Specify the layer 2 interface name.</li> </ul>                                                                                                          |
| ge <1-X>           | Clears MAC address forwarding table for the specified GigabitEthernet interface <ul style="list-style-type: none"> <li>• &lt;1-X&gt; – Specify the GigabitEthernet interface index from 1 - X.</li> </ul> <p><b>Note:</b> The number of GE interfaces supported varies for different device types.</p>     |
| port-channel <1-X> | Clears MAC address forwarding table for the specified port-channel interface <ul style="list-style-type: none"> <li>• &lt;1-X&gt; – Specify the port-channel interface index from 1 - X.</li> </ul> <p><b>Note:</b> The number of port-channel interfaces supported varies for different device types.</p> |
| on <DEVICE-NAME>   | Optional. Clears the MAC address forwarding table, for the selected interface, on a specified device <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul>                                                       |

```
clear mac-address-table mac-auth-state address <MAC> vlan <1-4904> {on <DEVICE-NAME>}
```



|                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mac-address-table mac-auth-state address <MAC> vlan <1-4904> | <p>Clears MAC addresses learned from a particular VLAN when WLAN MAC authentication and captive-portal fall back is enabled. Access points/controllers provide WLAN access to clients whose MAC address has been learned and stored in their MAC address tables. Use this command to clear a specified MAC address on the MAC address table. Once cleared the client has to re-authenticate, and is provided access only on successful authentication.</p> <ul style="list-style-type: none"> <li>• &lt;MAC&gt; - Specify the MAC address to clear. <ul style="list-style-type: none"> <li>• vlan &lt;1-4904&gt; - Specify the VLAN interface from 1 - 4094. In the AP/controller's MAC address table, the specified MAC address is cleared on the specified VLAN interface.</li> </ul> </li> </ul> |
| on <DEVICE-NAME>                                             | <p>Optional. Clears the specified MAC address on a specified device</p> <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> <p><b>Note:</b> If a device is not specified, the system clears the MAC address on all devices.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

```
clear mint mlcp history {on <DEVICE-NAME>}
```

|                  |                                                                                                                                                                                                                   |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mint             | Clears MINT related information                                                                                                                                                                                   |
| mlcp history     | Clears <i>MiNT Link Creation Protocol</i> (MLCP) client history                                                                                                                                                   |
| on <DEVICE-NAME> | <p>Optional. Clears MLCP client history on a specified device</p> <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
clear role ldap-stats {on <DEVICE-NAME>}
```

|                  |                                                                                                                                                                                                                      |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| role ldap-stats  | Clears LDAP (Lightweight Directory Access Protocol) server statistics                                                                                                                                                |
| on <DEVICE-NAME> | <p>Optional. Clears LDAP server statistics on a specified device</p> <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
clear rtls [aer scout|ekahau] {<MAC/DEVICE-NAME> {on <DEVICE-OR-DOMAIN-NAME>}|
on <DEVICE-OR-DOMAIN-NAME>}
```

|           |                                                     |
|-----------|-----------------------------------------------------|
| rtls      | Clears RTLS (Real Time Location Service) statistics |
| aer scout | Clears RTLS Aer scout statistics                    |
| ekahau    | Clears RTLS Ekahau statistics                       |

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <MAC/DEVICE-NAME>          | <p>This keyword is common to the 'aeroscout' and 'ekahau' parameters.</p> <ul style="list-style-type: none"> <li>• &lt;MAC/DEVICE-NAME&gt; – Optional. Clears Aeroscout or Ekahau RTLS statistics on a specified AP, wireless controller, or service platform. Specify the AP's MAC address or hostname.</li> </ul>                                                                                                      |
| on <DEVICE-OR-DOMAIN-NAME> | <p>This keyword is common to the 'aeroscout' and 'ekahau' parameters.</p> <ul style="list-style-type: none"> <li>• on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Clears Aeroscout or Ekahau RTLS statistics on a specified AP, wireless controller, service platform, or RF Domain</li> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> |

```
clear spanning-tree detected-protocols {on <DEVICE-NAME>}
```

|                    |                                                                                                                                                                                                                     |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| spanning-tree      | Clears spanning tree entries on an interface and restarts protocol migration                                                                                                                                        |
| detected-protocols | Restarts protocol migration                                                                                                                                                                                         |
| on <DEVICE-NAME>   | <p>Optional. Clears spanning tree entries on a specified device</p> <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
clear spanning-tree detected-protocols {interface [<INTERFACE-NAME>|ge <1-X>|me1|port-channel <1-X>|pppoe1|up1|vlan <1-4094>|wwan1]} {on <DEVICE-NAME>}
```

|                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| spanning-tree                                                                                    | Clears spanning tree entries on an interface and restarts protocol migration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| detected-protocols                                                                               | Restarts protocol migration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| interface [<INTERFACE-NAME>  ge <1-X> me1  port-channel <1-X>  pppoe1 up1  vlan <1-4094>  wwan1] | <p>Optional. Clears spanning tree entries on different interfaces</p> <ul style="list-style-type: none"> <li>• &lt;INTERFACE-NAME&gt; – Clears detected spanning tree entries on a specified interface. Specify the interface name.</li> <li>• ge &lt;1-X&gt; – Clears detected spanning tree entries for the selected GigabitEthernet interface. Select the GigabitEthernet interface index from 1 - X.</li> <li>• me1 – Clears FastEthernet interface spanning tree entries</li> <li>• port-channel &lt;1-X&gt; – Clears detected spanning tree entries for the selected port channel interface. Select the port channel index from 1 - X. The number of port-channel interfaces supported varies for different device types.</li> <li>• pppoe1 – Clears detected spanning tree entries for PPPoE (Point-to-Point Protocol over Ethernet) interface</li> <li>• up1 – Clears detected spanning tree entries for the WAN Ethernet interface</li> <li>• vlan &lt;1-4094&gt; – Clears detected spanning tree entries for the selected VLAN interface. Select a SVI (Switch Virtual Interface) VLAN ID from 1- 4094.</li> <li>• wwan1 – Clears detected spanning tree entries for wireless WAN interface.</li> </ul> |
| on <DEVICE-NAME>                                                                                 | <p>Optional. Clears spanning tree entries on a specified device</p> <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

```
clear traffic-shape statistics class <1-4> {(on <DEVICE-NAME>)}
```

|                          |                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| traffic-shape statistics | Clears traffic shaping statistics                                                                                                                                                                                                                                                                                                                                                  |
| class <1-4>              | Clears traffic shaping statistics for a specific traffic class <ul style="list-style-type: none"> <li>• &lt;1-4&gt; - Specify the traffic class from 1 - 4.</li> </ul> <p><b>Note:</b> If the traffic class is not specified, the system clears all traffic shaping statistics.</p>                                                                                                |
| on <DEVICE-NAME>         | Optional. Clears traffic shaping statistics for the specified traffic class on a specified device <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the access point, wireless controller, or service platform.</li> </ul> <p><b>Note:</b> For more information on configuring traffic-shape, see <a href="#">traffic-shape</a> on page 1224.</p> |

```
clear vrrp [error-stats|stats] {on <DEVICE-NAME>}
```

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vrrp             | Clears VRRP ( <i>Virtual Router Redundancy Protocol</i> ) statistics<br>VRRP allows a pool of routers to be advertised as a single virtual router. This virtual router is configured by hosts as their default gateway. VRRP elects a master router, from this pool, and assigns it a virtual IP address. The master router routes and forwards packets to hosts on the same subnet. When the master router fails, one of the backup routers is elected as the master and its IP address is mapped to the virtual IP address. |
| error-stats      | Clears global error statistics                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| stats            | Clears VRRP related statistics                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| on <DEVICE-NAME> | This following keywords are common to the 'error-stats' and 'stats' parameters: <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; - Optional. Clears VRRP statistics on a specified device</li> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul>                                                                                                                                                                                                    |

### Examples (User Exec Mode)

```
rfs4000-229D58>clear event-history
rfs4000-229D58>clear spanning-tree detected-protocols interface port-channel 1
rfs4000-229D58>clear spanning-tree detected-protocols interface ge 1
NOC-NX9500>show lldp neighbors

Chassis ID: 00-18-71-D0-0B-00
System Name: ProCurve Switch 5406z1
Platform: ProCurve J8697A Switch 5406z1, revision K.12.1X, ROM K.11.03 (/sw/code/build/btm(sw_espl))
Capabilities: Bridge Router
Enabled Capabilities: Bridge Router
Local Interface: ge1, Port ID(Port Description) (outgoing port): 26(B2)
TTL: 95 sec
Management Addresses: 10.234.160.1

Chassis ID: 5C-0E-8B-1C-53-2C
System Name: HM-ROUTER
Platform: RFS-4011-11110-WR, Version 5.9.1.0-016D
Capabilities: Bridge WLAN Access Point Router
Enabled Capabilities: Bridge WLAN Access Point Router
Local Interface: ge2, Port ID(Port Description) (outgoing port): ge1(ge1)
TTL: 165 sec
```

Management Addresses: 192.168.0.1,172.168.16.1,192.168.13.1,20.168.10.1

NOC-NX9500>

NOC-NX9500>clear lldp neighbors

NOC-NX9500>show lldp neighbors

NOC-NX9500>

NOC-NX9500>show cdp neighbors

| Device ID | Platform          | Local Interface | Port ID | Duplex |
|-----------|-------------------|-----------------|---------|--------|
| HM-ROUTER | RFS-4011-11110-WR | ge2             | ge1     | full   |

NOC-NX9500>

NOC-NX9500>clear cdp neighbors

NOC-NX9500>show cdp neighbors

| Device ID | Platform | Local Interface | Port ID | Duplex |
|-----------|----------|-----------------|---------|--------|
|-----------|----------|-----------------|---------|--------|

NOC-NX9500>

rfs4000-229D58>clear role ldap-stats

rfs4000-229D58>show role ldap-stats

No ROLE LDAP statistics found.

rfs4000-229D58>

rfs4000-229D58>show mac-address-table

| BRIDGE | VLAN | PORT | MAC               | STATE   |
|--------|------|------|-------------------|---------|
| 1      | 1    | ge5  | 00-02-B3-28-D1-55 | forward |
| 1      | 1    | ge5  | 00-0F-8F-19-BA-4C | forward |
| 1      | 1    | ge5  | B4-C7-99-5C-FA-8E | forward |
| 1      | 1    | ge5  | 00-23-68-0F-43-D8 | forward |
| 1      | 1    | ge5  | 00-15-70-38-06-49 | forward |
| 1      | 1    | ge5  | 00-23-68-13-9B-34 | forward |
| 1      | 1    | ge5  | B4-C7-99-58-72-58 | forward |
| 1      | 1    | ge5  | 00-15-70-81-74-2D | forward |

Total number of MACs displayed: 8

rfs4000-229D58>

rfs4000-229D58>clear mac-address-table address 00-02-B3-28-D1-55

rfs4000-229D58>show mac-address-table

| BRIDGE | VLAN | PORT | MAC               | STATE   |
|--------|------|------|-------------------|---------|
| 1      | 1    | ge5  | 00-0F-8F-19-BA-4C | forward |
| 1      | 1    | ge5  | B4-C7-99-5C-FA-8E | forward |
| 1      | 1    | ge5  | 00-23-68-0F-43-D8 | forward |
| 1      | 1    | ge5  | 00-15-70-38-06-49 | forward |
| 1      | 1    | ge5  | 00-23-68-13-9B-34 | forward |
| 1      | 1    | ge5  | B4-C7-99-58-72-58 | forward |
| 1      | 1    | ge5  | 00-15-70-81-74-2D | forward |

Total number of MACs displayed: 7

rfs4000-229D58>

### Examples (Priv-Exec-Mode)

NOC-NX9500#show event-history

EVENT HISTORY REPORT

Generated on '2017-12-21 10:30:56 IST' by 'admin'

|                                                    |            |        |               |                        |
|----------------------------------------------------|------------|--------|---------------|------------------------|
| 2017-12-21 10:30:48                                | NOC-NX9500 | SYSTEM | LOGIN         | Successfully logged in |
| user 'admin' with privilege 'superuser' from 'ssh' |            |        |               |                        |
| 2017-12-21 10:28:57                                | NOC-NX9500 | DIAG   | PWRSPPLY_FAIL | Power supply           |
| redundancy failure                                 |            |        |               |                        |

```

2017-12-21 10:18:55 NOC-NX9500 DIAG PWRSPPLY_FAIL Power supply
redundancy failure
2017-12-21 10:08:52 NOC-NX9500 DIAG PWRSPPLY_FAIL Power supply
redundancy failure
2017-12-21 09:58:49 NOC-NX9500 DIAG PWRSPPLY_FAIL Power supply
redundancy failure
2017-12-21 09:48:46 NOC-NX9500 DIAG PWRSPPLY_FAIL Power supply
redundancy failure

```

```

--More--
NOC-NX9500#
NOC-NX9500#clear event-history
NOC-NX9500#show event-history
EVENT HISTORY REPORT
Generated on '2017-12-21 10:32:25 IST' by 'admin'

```

```

NOC-NX9500#
NOC-NX9500#show mac-address-table

```

| BRIDGE   | VLAN     | PORT       | MAC                      | STATE          |
|----------|----------|------------|--------------------------|----------------|
| 1        | 1        | ge1        | 00-18-71-D0-1B-E6        | forward        |
| 1        | 1        | ge1        | 74-67-F7-07-02-35        | forward        |
| 1        | 1        | ge1        | 84-24-8D-84-A2-24        | forward        |
| 1        | 1        | ge1        | 00-04-96-9C-F1-25        | forward        |
| 1        | 1        | ge1        | 84-24-8D-DF-9A-4C        | forward        |
| <b>1</b> | <b>1</b> | <b>ge1</b> | <b>B4-C7-99-71-17-28</b> | <b>forward</b> |

```

Total number of MACs displayed: 6
NOC-NX9500#
NOC-NX9500#clear mac-address-table address B4-C7-99-71-17-28
NOC-NX9500#commit
NOC-NX9500#write memory
NOC-NX9500#show mac-address-table

```

| BRIDGE | VLAN | PORT | MAC               | STATE   |
|--------|------|------|-------------------|---------|
| 1      | 1    | ge1  | 00-18-71-D0-1B-E6 | forward |
| 1      | 1    | ge1  | 74-67-F7-07-02-35 | forward |
| 1      | 1    | ge1  | 84-24-8D-84-A2-24 | forward |
| 1      | 1    | ge1  | 00-04-96-9C-F1-25 | forward |
| 1      | 1    | ge1  | 84-24-8D-DF-9A-4C | forward |

```

Total number of MACs displayed: 5
NOC-NX9500#

```

### clock (user and privi exec modes)

Sets a device's system clock. By default all WiNG devices are shipped with the time zone and time format set to UTC and 24-hour clock respectively. If a device's clock is set without resetting the time zone, the time is displayed relative to the UTC (Universal Time Coordinated) - Greenwich Time. To display time in the local time zone format, in the device's configuration mode, use the `timezone` command. You can also reset the time zone at the RF Domain level. When configured as RF Domain setting, it applies to all devices within the domain. Configuring the local time zone prior to setting the clock is recommended. For more information on configuring RF Domain time zone, see [timezone](#).



#### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
clock set <HH:MM:SS> <1-31> <MONTH> <1993-2035> {on <DEVICE-NAME>}
```

### Parameters

```
clock set <HH:MM:SS> <1-31> <MONTH> <1993-2035> {on <DEVICE-NAME>}
```

|                  |                                                                                                                                                                                                     |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| clock set        | Sets a device's software system clock                                                                                                                                                               |
| <HH:MM:SS>       | Sets the current time (in military format hours, minutes, and seconds)<br><br><b>Note:</b> By default, the WiNG software displays time in the 24-hour clock format. This setting cannot be changed. |
| <1-31>           | Sets the numerical day of the month                                                                                                                                                                 |
| <MONTH>          | Sets the month of the year (Jan to Dec)                                                                                                                                                             |
| <1993-2035>      | Sets a valid four digit year from 1993 - 2035                                                                                                                                                       |
| on <DEVICE-NAME> | Optional. Sets the clock on a specified device <ul style="list-style-type: none"><li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li></ul>        |

### Examples (User Exec Mode)

The following commands set the time zone and clock for the logged device:

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#timezone America/Los_Angeles
nx9500-6C8809>clock set 11:24:30 21 Jan 2017
nx9500-6C8809>show clock
2017-01-21 12:14:14 PST
nx9500-6C8809>
```

Note, if the clock is set without resetting the time zone, the time displays as UTC time, as shown in the following example:

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#no timezone
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#commit
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show clock
2017-01-21 19:15:55 UTC

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```

### Examples (Privileged Exec Mode)

```
ap8432-070235(config-device-74-67-F7-07-02-35)#timezone America/Los_Angeles
ap8432-070235#clock set 12:51:10 21 Dec 2017
ap8432-070235#show clock
2017-12-21 04:52:06 PST
ap8432-070235#
```

## cluster (user and privi exec modes)

Initiates cluster context. The cluster context provides centralized management to configure all cluster members from any one member. Commands executed under this context are executed on all members of the cluster.



### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
cluster start-election
```

### Parameters

```
cluster start-election
```

|                |                                      |
|----------------|--------------------------------------|
| start-election | Starts a new cluster master election |
|----------------|--------------------------------------|

### Examples (User Exec Mode)

```
nx9500-6C8809>cluster start-election
nx9500-6C8809>
```

### Examples (Privi Exec Mode)

```
rfs4000-229D58#cluster start-election
rfs4000-229D58#
```

### Related Commands

|                                                                       |                                                                                                    |
|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| <a href="#">create-cluster (user and privi exec modes)</a> on page 47 | Creates a new cluster on the specified device                                                      |
| <a href="#">join-cluster (user and privi exec modes)</a> on page 77   | Adds a wireless controller or service platform, as a member, to an existing cluster of controllers |

## configure

Enters the configuration mode. Use this command to enter the current device's configuration mode, or enable configuration from the terminal.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
configure {self|terminal}
```

## Parameters

configure {self|terminal}

|          |                                                             |
|----------|-------------------------------------------------------------|
| self     | Optional. Enables the logged-in device's configuration mode |
| terminal | Optional. Enables configuration from the terminal           |

## Examples

```
nx9500-6C8809#configure self
Enter configuration commands, one per line. End with CNTL/Z.
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
NOC-NX9500#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
NOC-NX9500(config)#
```

*connect (user and privi exec modes)*

Begins a console connection to a remote device using the remote device's MiNT ID or name



### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

## Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
connect [mint-id <MINT-ID>|<REMOTE-DEVICE-NAME>]
```

## Parameters

```
connect [mint-id <MINT-ID>|<REMOTE-DEVICE-NAME>]
```

|                      |                                                                                                                                                               |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mint-id <MINT-ID>    | Connects to the remote system using its MiNT ID <ul style="list-style-type: none"><li>• &lt;MINT-ID&gt; - Specify the remote device's MiNT ID.</li></ul>      |
| <REMOTE-DEVICE-NAME> | Connects to the remote system using its name <ul style="list-style-type: none"><li>• &lt;REMOTE-DEVICE-NAME&gt; - Specify the remote device's name.</li></ul> |

## Examples (User Exec Mode)

```
NOC-NX9500>show mint lsp-db
5 LSPs in LSP-db of 19.6C.88.09:
LSP 19.6C.88.09 at level 1, hostname "NOC-NX9500", 2 adjacencies, seqnum 1518782
LSP 19.6D.B5.D4 at level 1, hostname "RFS6K-SITE2-VLAN192", 2 adjacencies, seqnum 1971569
LSP 19.74.B4.5C at level 1, hostname "ap8132-74B45C", 1 adjacencies, seqnum 1741167
LSP 4D.83.30.A4 at level 1, hostname "ap7522-8330A4", 1 adjacencies, seqnum 518868
LSP 70.38.06.49 at level 1, hostname "RFS6K-SITE1-VLAN20", 2 adjacencies, seqnum 1389974
NOC-NX9500>
NOC-NX9500>connect mint-id 19.74.B4.5C
```

```
Entering character mode
Escape character is '^']'.
```



```
AP8432 release 5.9.2.0-029R
ap8432-74B45C login:
```

### Examples (Privi Exec Mode)

```
nx9500-6C8809#connect mint-id ?
MINT-ID MINT ID of device to connect to
```

```
nx9500-6C8809#connect mint-id 19.22.9D.58
```

```
Entering character mode
Escape character is '^']'.
```

```
RFS4000 release 5.9.2.0-012D
rfs4000-229D58 login: admin
Password:
rfs4000-229D58>
```

### copy

Copies a file (config,log,txt...etc) from any location to the Access Point, wireless controller, or service platform and vice-versa

#### Note



Copying a new config file to an existing running-config file merges it with the existing running-config file on the wireless controller. Both the existing running-config and the new config file are applied as the current running-config. Copying a new config file to a start-up config file replaces the existing start-up config file with the parameters of the new file. It is better to erase the existing start-up config file and then copy the new config file to the startup config.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
copy [<SOURCE-FILE>|<SOURCE-URL>] [<DESTINATION-FILE>|<DESTINATION-URL>]
```

#### Parameters

```
copy [<SOURCE-FILE>|<SOURCE-URL>] [<DESTINATION-FILE>|<DESTINATION-URL>]
```

|                    |                                                |
|--------------------|------------------------------------------------|
| <SOURCE-FILE>      | Specify the source file to copy.               |
| <SOURCE-URL>       | Specify the source file's location (URL).      |
| <DESTINATION-FILE> | Specify the destination file to copy to.       |
| <DESTINATION-URL>  | Specify the destination file's location (URL). |

## Examples

Transferring file snmpd.log to remote TFTP server.

```
rfs4000-229D58#copy flash:/log/snmpd.log tftp://10.233.89.183:/snmpd.log
Accessing running-config file from remote TFTP server into switch running-config.
rfs4000-229D58#copy tftp://10.233.89.183:/running-config running-config
```

*cpe (privilege-exec-mode)*

Enables a WiNG controller to perform certain operations on CPEs (Customer Premises Equipments) through an adopted T5 controller

A T5 controller uses the IPX operating system to manage its connected radio devices, as opposed to the WiNG operating system used by RFS wireless controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The CPEs are the T5 controller managed radio devices using the IPX operating system. These CPEs use a DSL (Digital Subscriber Line) as their high speed Internet access mechanism using the CPE's physical wallplate connection and phone jack.

### Supported in the following platforms:

- Wireless Controllers — RFS 4000, RFS 6000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
cpe [boot|reload|upgrade]
cpe boot system cpe [<1-24>|all] [primary|secondary] {on <T5-DEVICE-NAME>}
cpe [reload|upgrade <IMAGE-LOCATION>] cpe [<1-24>|all] {on <T5-DEVICE-NAME>}
```



#### Note

These commands can also be executed on the T5 profile and device context. For more information, see [T5 Profile Config Commands](#) on page 1285.

### Parameters

```
cpe boot system cpe [<1-24>|all] [primary|secondary] {on <T5-DEVICE-NAME>}
```

|                     |                                                                                                                                                                                                                                                |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cpe boot system     | Changes the image used by a CPE to boot. When reloading, the CPE uses the specified image.                                                                                                                                                     |
| cpe [<1-24> all]    | Identifies the CPE(s) on which this change is implemented <ul style="list-style-type: none"><li>• &lt;1-24&gt; - Reloads only those CPEs whose IDs have been specified. Specify the ID from 1 - 24.</li><li>• all - Reloads all CPEs</li></ul> |
| [primary secondary] | Select the next boot image <ul style="list-style-type: none"><li>• primary - Uses the primary image when reloading</li><li>• secondary - Uses the secondary image when reloading</li></ul>                                                     |
| on <T5-DEVICE-NAME> | Optional. Performs this operation on a specified T5 device <ul style="list-style-type: none"><li>• &lt;T5-DEVICE-NAME&gt; - Specify the T5 device's hostname.</li></ul>                                                                        |

```
cpe [reload|upgrade <IMAGE-LOCATION>] cpe [<1-24>|all] {on <T5-DEVICE-NAME>}
```

|                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cpe [reload  upgrade<br><IMAGE-LOCATION>] | <p>Performs the following operations on CPEs</p> <ul style="list-style-type: none"> <li>• reload - Reloads the device</li> <li>• upgrade &lt;IMAGE-LOCATION&gt; - Upgrades the device</li> <li>• &lt;IMAGE-LOCATION&gt; - Specify the location of the firmware image. Both IPv4 and IPv6 addresses are supported.</li> </ul> <p>Use one of the following options to provide the location:</p> <p>IPv4 URLs:</p> <ul style="list-style-type: none"> <li>• tftp://&lt;hostname IP&gt;[:port]/path/file</li> <li>• ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IP&gt;[:port]/path/file</li> <li>• sftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IP&gt;[:port]/path/file</li> <li>• http://&lt;hostname IP&gt;[:port]/path/file cf:/path/file usb&lt;n&gt;:/path/file</li> </ul> <p>IPv6 URLs:</p> <ul style="list-style-type: none"> <li>• tftp://&lt;hostname [IPv6]&gt;[:port]/path/file</li> <li>• ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname [IPv6]&gt;[:port]/path/file</li> <li>• sftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname [IPv6]&gt;[:port]/path/file</li> <li>• http://&lt;hostname [IPv6]&gt;[:port]/path/file</li> </ul> <p><b>Note:</b> After specifying the operation to perform, identify the device(s).</p> |
| cpe [<1-24> all]                          | <p>Identifies the CPE(s) on which the operation is performed</p> <ul style="list-style-type: none"> <li>• &lt;1-24&gt; - Configures the CPE's ID from 1 - 24</li> <li>• all - Configures all CPEs</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| on <T5-DEVICE-NAME>                       | <p>Optional. Performs this operation on a specified T5 device</p> <ul style="list-style-type: none"> <li>• &lt;T5-DEVICE-NAME&gt; - Specify the T5 device's hostname.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

### Example

```
nx9500-6C8809#show t5 cpe boot on t5-ED7C6C
```

```

 DEVICE PRIMARY VERSION SECONDARY VERSION NEXT BOOT UPGRADE STATUS UPGRADE
 PROGRESS %

 cpe1 5.4.2.0-010R 5.4.2.0-006B primary none 0
 cpe2 5.4.2.0-010R 5.4.2.0-006B primary none 0

```

```
nx9500-6C8809#
nx9500-6C8809#cpe boot system cpe 1 secondary on t5-ED7C6C
Updated T5 CPE system boot partition
nx9500-6C8809#
```

### *create-cluster (user and privi exec modes)*

Creates a new device cluster, with the specified name, and assigns it an IP address and routing level

A cluster (or redundancy group) is a set of controllers or service platforms (nodes) uniquely defined by a profile configuration. Within the cluster, members discover and establish connections to other members and provide wireless network self-healing support in the event of member's failure.

A cluster's load balance is typically distributed evenly amongst its members. An administrator needs to define how often the profile is load balanced for radio distribution, as radios can come and go and members join and exit the cluster.



#### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

#### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
create-cluster name <CLUSTER-NAME> ip <IP> {level [1|2]}
```

#### Parameters

```
create-cluster name <CLUSTER-NAME> ip <IP> {level [1|2]}
```

|                     |                                                                                                                                                                                                                                                                              |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| create-cluster      | Creates a cluster                                                                                                                                                                                                                                                            |
| name <CLUSTER-NAME> | Configures the cluster name <ul style="list-style-type: none"><li>• &lt;CLUSTER-NAME&gt; - Specify a cluster name. Define a name for the cluster that uniquely identifies its configuration or profile support requirements. The name cannot exceed 64 characters.</li></ul> |
| ip <IP>             | Specifies the device's IP address used for cluster creation <ul style="list-style-type: none"><li>• &lt;IP&gt; - Specify the device's IP address in the A.B.C.D format.</li></ul>                                                                                            |
| level [1 2]         | Optional. Configures the routing level for this cluster <ul style="list-style-type: none"><li>• 1 - Configures level 1 (local) routing</li><li>• 2 - Configures level 2 (inter-site) routing</li></ul>                                                                       |

#### Examples (User Exec Mode)

```
rfs4000-6DB5D4>create-cluster name TechPubs ip 192.168.13.23 level 1
... creating cluster
... committing the changes
... saving the changes
Please Wait .
[OK]
rfs4000-6DB5D4>
rfs4000-6DB5D4>show context session-config include-factory | include cluster name TechPubs
 cluster name TechPubs
rfs4000-6DB5D4>
```

#### Examples (Priv Exec Mode)

```
rfs4000-229D58#create-cluster name TechPubs1 ip 192.168.13.8 level 2
... creating cluster
... committing the changes
... saving the changes
Please Wait .
[OK]
rfs4000-229D58#
rfs4000-229D58#show cluster configuration
```

---

#### Cluster Configuration Information

```
Name : TechPubs1
Configured Mode : Active
Master Priority : 128
Force configured state : Disabled
Force configured state delay : 5 minutes
Handle STP : Disabled
Radius Counter DB Sync Time : 5 minutes
rfs4000-229D58#
```

#### Related Commands

|                                                                     |                                                                                                                                      |
|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">cluster (user and privi exec modes)</a> on page 46      | Initiates cluster context. The cluster context provides centralized management to configure all cluster members from any one member. |
| <a href="#">join-cluster (user and privi exec modes)</a> on page 77 | Adds a wireless controller or service platform, as a member, to an existing cluster of controllers                                   |

#### *crypto (user and privi exec modes)*

Enables digital certificate configuration and RSA Keypair management. Digital certificates are issued by CAs and contain user or device specific information, such as name, public key, IP address, serial number, company name etc. Use this command to generate, delete, export, or import encrypted RSA Keypairs and generate *Certificate Signing Request (CSR)*.

This command also enables trustpoint configuration. Trustpoints contain the CA's identity and configuration parameters.



#### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

---

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
crypto [key|pki]
crypto key [export|generate|import|zeroize]
crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL> {background/on/passphrase}
crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL>
{background/passphrase <KEY-PASSPHRASE> background} {(on <DEVICE-NAME>)}
crypto key generate rsa <RSA-KEYPAIR-NAME> [2048|4096] {on <DEVICE-NAME>}
crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL> {background/on/passphrase}
crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL>
{background/passphrase <KEY-PASSPHRASE> background} {(on <DEVICE-NAME>)}
crypto key zeroize rsa <RSA-KEYPAIR-NAME> {force} {(on <DEVICE-NAME>)}
crypto pki [authenticate|export|generate|import|zeroize]
crypto pki authenticate <TRUSTPOINT-NAME> <LOCATION-URL> {background} {(on <DEVICE-NAME>)}
crypto pki export [request|trustpoint]
crypto pki export request [generate-rsa-key|short|use-rsa-key] <RSA-KEYPAIR-NAME>
[autogen-subject-name|subject-name]
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME>
autogen-subject-name [<EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>]
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME>
autogen-subject-name (<EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>)
crypto pki export request [generate-rsa-key|short [generate-rsa-key|use-rsa-key]|use-rsa-
key]
<RSA-KEYPAIR-NAME> subject-name <COMMON-NAME> <COUNTRY> <STATE> <CITY> <ORGANIZATION>
<ORGANIZATION-UNIT> (<EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>)
crypto pki export trustpoint <TRUSTPOINT-NAME> <EXPORT-TO-URL> {background/passphrase <KEY-
PASSPHRASE> background}
{(on <DEVICE-NAME>)}
crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key]
<RSA-KEYPAIR-NAME> [autogen-subject-name|subject-name]
crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key]
<RSA-KEYPAIR-NAME> autogen-subject-name {(email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address
<IP>,
on <DEVICE-NAME>)}
crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key]
<RSA-KEYPAIR-NAME> subject-name <COMMON-NAME> <COUNTRY> <STATE> <CITY> <ORGANIZATION>
<ORGANIZATION-UNIT> {(email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>,on <DEVICE-NAME>)}
crypto pki import [certificate|crl|trustpoint]
crypto pki import [certificate|crl] <TRUSTPOINT-NAME> <IMPORT-FROM-URL> {background} {(on
<DEVICE-NAME>)}
crypto pki import trustpoint <TRUSTPOINT-NAME> <IMPORT-FROM-URL> {background/passphrase
<KEY-PASSPHRASE> background} {(on <DEVICE-NAME>)}
crypto pki zeroize trustpoint <TRUSTPOINT-NAME> {del-key} {(on <DEVICE-NAME>)}
```

## Parameters

```
crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL> {background/passphrase <KEY-
PASSPHRASE> background} {(on <DEVICE-NAME>)}
```

|                               |                                                                                                                                                                                                                                                   |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| key                           | Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.                                                                                                                                                |
| export rsa <RSA-KEYPAIR-NAME> | Exports an existing RSA Keypair to a specified destination <ul style="list-style-type: none"> <li>&lt;RSA-KEYPAIR-NAME&gt; - Specify the RSA Keypair name.</li> </ul>                                                                             |
| <EXPORT-TO-URL>               | Specify the RSA Keypair destination address. Both IPv4 and IPv6 address formats are supported. After specifying the destination address (where the RSA Keypair is exported), configure one of the following parameters: background or passphrase. |
| background                    | Optional. Performs export operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the export on.                                                                     |

|                                           |                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| passphrase <KEY-PASSPHRASE><br>background | Optional. Encrypts RSA Keypair before exporting <ul style="list-style-type: none"> <li>• &lt;KEY-PASSPHRASE&gt; – Specify a passphrase to encrypt the RSA Keypair.</li> <li>• background – Optional. Performs export operation in the background. After specifying the passphrase, optionally specify the device (access point or controller) to perform the export on.</li> </ul> |
| on <DEVICE-NAME>                          | The following parameter is recursive and common to all of the above parameters: <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; – Optional. Performs export operation on a specified device</li> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul>                                                      |

```
crypto key generate rsa <RSA-KEYPAIR-NAME> [2048|4096] {on <DEVICE-NAME>}
```

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| key                                         | Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.                                                                                                                                                                                                                                                                                                       |
| generate rsa <RSA-KEYPAIR-NAME> [2048 4096] | Generates a new RSA Keypair <ul style="list-style-type: none"> <li>• &lt;RSA-KEYPAIR-NAME&gt; – Specify the RSA Keypair name.</li> <li>• [2048 4096] – Sets the size of the RSA key in bits. The options are 2048 bits and 4096 bits. The default size is 2048 bits.</li> </ul> <p>After specifying the key size, optionally specify the device (access point or controller) to generate the key on.</p> |
| on <DEVICE-NAME>                            | Optional. Generates the new RSA Keypair on a specified device <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul>                                                                                                                                                                                            |

```
crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL>
{background|passphrase <KEY-PASSPHRASE> background} {(on <DEVICE-NAME>)}
```

|                               |                                                                                                                                                                                                                                              |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| key                           | Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.                                                                                                                                           |
| import rsa <RSA-KEYPAIR-NAME> | Imports a RSA Keypair from a specified source <ul style="list-style-type: none"> <li>• &lt;RSA-KEYPAIR-NAME&gt; – Specify the RSA Keypair name.</li> </ul>                                                                                   |
| <IMPORT-FROM-URL>             | Specify the RSA Keypair source address. Both IPv4 and IPv6 address formats are supported. After specifying the source address (where the RSA Keypair is imported from), configure one of the following parameters: background or passphrase. |
| background                    | Optional. Performs import operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the import on.                                                                |

|                                           |                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| passphrase <KEY-PASSPHRASE><br>background | Optional. Decrypts the RSA Keypair after importing <ul style="list-style-type: none"> <li>• &lt;KEY-PASSPHRASE&gt; - Specify the passphrase to decrypt the RSA Keypair.</li> <li>• background - Optional. Performs import operation in the background. After specifying the passphrase, optionally specify the device (access point, controller, or service platform) to perform the import on.</li> </ul> |
| on <DEVICE-NAME>                          | The following parameter is recursive and common to the 'background' and 'passphrase' keywords: <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; - Optional. Performs import operation on a specific device</li> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul>                                                                |

```
crypto key zeroize rsa <RSA-KEYPAIR-NAME> {force} {(on <DEVICE-NAME>)}
```

|                                |                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| key                            | Enables RSA Keypair management. Use this command to export, import, generate, or delete a RSA key.                                                                                                                                                                                                                              |
| zeroize rsa <RSA-KEYPAIR-NAME> | Deletes a specified RSA Keypair <ul style="list-style-type: none"> <li>• &lt;RSA-KEYPAIR-NAME&gt; - Specify the RSA Keypair name.</li> </ul> <p><b>Note:</b> All device certificates associated with this key will also be deleted.</p>                                                                                         |
| force                          | Optional. Forces deletion of all certificates associated with the specified RSA Keypair. Optionally specify a device on which to force certificate deletion.                                                                                                                                                                    |
| on <DEVICE-NAME>               | The following parameter is recursive and optional: <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; - Optional. Deletes all certificates associated with the RSA Keypair on a specified device</li> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
crypto pki authenticate <TRUSTPOINT-NAME> <URL> {background} {(on <DEVICE-NAME>)}
```

|                                |                                                                                                                                                                                                                                                                                                |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| pki                            | Enables Private Key Infrastructure (PKI) management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated Certificate Authority (CA) certificates.                                                                                                    |
| authenticate <TRUSTPOINT-NAME> | Authenticates a trustpoint and imports the corresponding CA certificate <ul style="list-style-type: none"> <li>• &lt;TRUSTPOINT-NAME&gt; - Specify the trustpoint name.</li> </ul>                                                                                                             |
| url                            | Specify CA's location. Both IPv4 and IPv6 address formats are supported. <p><b>Note:</b> The CA certificate is imported from the specified location.</p>                                                                                                                                       |
| background                     | Optional. Performs authentication in the background. If selecting this option, you can optionally specify the device (access point, controller, or service platform) to perform the export on.                                                                                                 |
| on <DEVICE-NAME>               | The following parameter is recursive and optional: <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; - Optional. Performs authentication on a specified device</li> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME>
autogen-subject-name (<EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>)
```



|                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| pki                                                       | Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.                                                                                                                                                                                                                                                                                                                                 |
| export request                                            | Exports CSR to the CA for digital identity certificate. The CSR contains applicant's details and RSA Keypair's public key.                                                                                                                                                                                                                                                                                                                                             |
| [generate-rsa-key <br>use-rsa-key] <RSA-<br>KEYPAIR-NAME> | Generates a new RSA Keypair or uses an existing RSA Keypair <ul style="list-style-type: none"> <li>• generate-rsa-key – Generates a new RSA Keypair for digital authentication</li> <li>• use-rsa-key – Uses an existing RSA Keypair for digital authentication <ul style="list-style-type: none"> <li>• &lt;RSA-KEYPAIR-NAME&gt; – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name.</li> </ul> </li> </ul> |
| autogen-subject-<br>name                                  | Auto generates subject name from configuration parameters. The subject name identifies the certificate.                                                                                                                                                                                                                                                                                                                                                                |
| <EXPORT-TO-URL>                                           | Specify the CA's location. Both IPv4 and IPv6 address formats are supported.<br><br><b>Note:</b> The CSR is exported to the specified location.                                                                                                                                                                                                                                                                                                                        |
| email <SEND-TO-<br>EMAIL>                                 | Exports CSR to a specified e-mail address <ul style="list-style-type: none"> <li>• &lt;SEND-TO-EMAIL&gt; – Specify the CA's e-mail address.</li> </ul>                                                                                                                                                                                                                                                                                                                 |
| fqdn <FQDN>                                               | Exports CSR to a specified Fully Qualified Domain Name (FQDN) <ul style="list-style-type: none"> <li>• &lt;FQDN&gt; – Specify the CA's FQDN.</li> </ul>                                                                                                                                                                                                                                                                                                                |
| ip-address <IP>                                           | Exports CSR to a specified device or system <ul style="list-style-type: none"> <li>• &lt;IP&gt; – Specify the CA's IP address.</li> </ul>                                                                                                                                                                                                                                                                                                                              |

```
crypto pki export request [generate-rsa-key|short [generate-rsa-key|use-rsa-key]|use-rsa-
key]
<RSA-KEYPAIR-NAME> subject-name <COMMON-NAME> <COUNTRY> <STATE> <CITY> <ORGANIZATION>
<ORGANIZATION-UNIT>
(<EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>)
```

|                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| pki                                                                                                 | Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| export request                                                                                      | Exports CSR to the CA for a digital identity certificate. The CSR contains applicant's details and RSA Keypair's public key.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| [generate-rsa-key  short<br>[generate-rsa-key use-rsa-<br>key]  use-rsa-key] <RSA-<br>KEYPAIR-NAME> | Generates a new RSA Keypair or uses an existing RSA Keypair <ul style="list-style-type: none"> <li>• generate-rsa-key – Generates a new RSA Keypair for digital authentication</li> <li>• short [generate-rsa-key use-rsa-key] – Generates and exports a shorter version of the CSR <ul style="list-style-type: none"> <li>• generate-rsa-key – Generates a new RSA Keypair for digital authentication. If generating a new RSA Keypair, specify a name for it.</li> <li>• use-rsa-key – Uses an existing RSA Keypair for digital authentication. If using an existing RSA Keypair, specify its name.</li> </ul> </li> <li>• use-rsa-key – Uses an existing RSA Keypair for digital authentication <ul style="list-style-type: none"> <li>• &lt;RSA-KEYPAIR-NAME&gt; – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name.</li> </ul> </li> </ul> |
| subject-name <COMMON-<br>NAME>                                                                      | Configures a subject name, defined by the <COMMON-NAME> keyword, to identify the certificate <ul style="list-style-type: none"> <li>• &lt;COMMON-NAME&gt; – Specify the common name used with the CA certificate. The name should enable you to identify the certificate easily (2 to 64 characters in length).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

|                       |                                                                                                                                                      |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <COUNTRY>             | Sets the deployment country code (2 character ISO code)                                                                                              |
| <STATE>               | Sets the state name (2 to 64 characters in length)                                                                                                   |
| <CITY>                | Sets the city name (2 to 64 characters in length)                                                                                                    |
| <ORGANIZATION>        | Sets the organization name (2 to 64 characters in length)                                                                                            |
| <ORGANIZATION-UNIT>   | Sets the organization unit (2 to 64 characters in length)                                                                                            |
| <EXPORT-TO-URL>       | Specify the CA's location. Both IPv4 and IPv6 address formats are supported. The CSR is exported to the specified location.                          |
| email <SEND-TO-EMAIL> | Exports CSR to a specified e-mail address <ul style="list-style-type: none"> <li>&lt;SEND-TO-EMAIL&gt; - Specify the CA's e-mail address.</li> </ul> |
| fqdn <FQDN>           | Exports CSR to a specified FQDN <ul style="list-style-type: none"> <li>&lt;FQDN&gt; - Specify the CA's FQDN.</li> </ul>                              |
| ip-address <IP>       | Exports CSR to a specified device or system <ul style="list-style-type: none"> <li>&lt;IP&gt; - Specify the CA's IP address.</li> </ul>              |

```
crypto pki export trustpoint <TRUSTPOINT-NAME> <EXPORT-TO-URL>
{background/passphrase <KEY-PASSPHRASE> background} {(on <DEVICE-NAME>)}
```

|                                           |                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| pki                                       | Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.                                                                                                                                                                                                                                                        |
| export trustpoint <TRUSTPOINT-NAME>       | Exports a trustpoint along with CA certificate, Certificate Revocation List (CRL), server certificate, and private key <ul style="list-style-type: none"> <li>&lt;TRUSTPOINT-NAME&gt; - Specify the trustpoint name (should be authenticated).</li> </ul>                                                                                                                                     |
| <EXPORT-TO-URL>                           | Specify the destination address. Both IPv4 and IPv6 address formats are supported. The trustpoint is exported to the address specified here.                                                                                                                                                                                                                                                  |
| background                                | Optional. Performs export operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the export on                                                                                                                                                                                                                  |
| passphrase <KEY-PASSPHRASE><br>background | Optional. Encrypts the key with a passphrase before exporting <ul style="list-style-type: none"> <li>&lt;KEY-PASSPHRASE&gt; - Specify the passphrase to encrypt the trustpoint.</li> <li>background - Optional. Performs export operation in the background. After specifying the passphrase, optionally specify the device (access point or controller) to perform the export on.</li> </ul> |
| on <DEVICE-NAME>                          | The following parameter is recursive and common to the 'background' and 'passphrase' keywords: <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; - Optional. Performs export operation on a specified device</li> <li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul>                                                      |

```
crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key]
<RSA-KEYPAIR-NAME> autogen-subject-name {(email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address
<IP>,
on <DEVICE-NAME>)}
```

|          |                                                                                                                                     |
|----------|-------------------------------------------------------------------------------------------------------------------------------------|
| pki      | Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated certificates. |
| generate | Generates a certificate and a trustpoint                                                                                            |

|                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| self-signed<br><TRUSTPOINT-NAME>                   | Generates a self-signed certificate and a trustpoint <ul style="list-style-type: none"> <li>• &lt;TRUSTPOINT-NAME&gt; – Specify a name for the certificate and its trustpoint.</li> </ul>                                                                                                                                                                                                                                                                               |
| [generate-rsa-key  use-rsa-key] <RSA-KEYPAIR-NAME> | Generates a new RSA Keypair, or uses an existing RSA Keypair <ul style="list-style-type: none"> <li>• generate-rsa-key – Generates a new RSA Keypair for digital authentication</li> <li>• use-rsa-key – Uses an existing RSA Keypair for digital authentication <ul style="list-style-type: none"> <li>• &lt;RSA-KEYPAIR-NAME&gt; – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name.</li> </ul> </li> </ul> |
| autogen-subject-name                               | Auto generates the subject name from the configuration parameters. The subject name helps to identify the certificate.                                                                                                                                                                                                                                                                                                                                                  |
| email <SEND-TO-EMAIL>                              | Optional. Exports the self-signed certificate to a specified e-mail address <ul style="list-style-type: none"> <li>• &lt;SEND-TO-EMAIL&gt; – Specify the e-mail address.</li> </ul>                                                                                                                                                                                                                                                                                     |
| fqdn <FQDN>                                        | Optional. Exports the self-signed certificate to a specified FQDN <ul style="list-style-type: none"> <li>• &lt;FQDN&gt; – Specify the FQDN.</li> </ul>                                                                                                                                                                                                                                                                                                                  |
| ip-address <IP>                                    | Optional. Exports the self-signed certificate to a specified device or system <ul style="list-style-type: none"> <li>• &lt;IP&gt; – Specify the device’s IP address.</li> </ul>                                                                                                                                                                                                                                                                                         |
| on <DEVICE-NAME>                                   | Optional. Exports the self-signed certificate on a specified device <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul>                                                                                                                                                                                                                                                     |

```
crypto pki generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key]
<RSA-KEYPAIR-NAME> subject-name <COMMON-NAME> <COUNTRY> <STATE> <CITY> <ORGANIZATION>
<ORGANIZATION-UNIT> { (email <SEND-TO-EMAIL>, fqdn <FQDN>, ip-address <IP>, on <DEVICE-NAME>) }
```

|                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| pki                                                | Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated certificates.                                                                                                                                                                                                                                                                                                                                     |
| generate self-signed<br><TRUSTPOINT-NAME>          | Generates a self-signed certificate and a trustpoint <ul style="list-style-type: none"> <li>• &lt;TRUSTPOINT-NAME&gt; – Specify a name for the certificate and its trustpoint.</li> </ul>                                                                                                                                                                                                                                                                               |
| [generate-rsa-key  use-rsa-key] <RSA-KEYPAIR-NAME> | Generates a new RSA Keypair, or uses an existing RSA Keypair <ul style="list-style-type: none"> <li>• generate-rsa-key – Generates a new RSA Keypair for digital authentication</li> <li>• use-rsa-key – Uses an existing RSA Keypair for digital authentication <ul style="list-style-type: none"> <li>• &lt;RSA-KEYPAIR-NAME&gt; – If generating a new RSA Keypair, specify a name for it. If using an existing RSA Keypair, specify its name.</li> </ul> </li> </ul> |
| subject-name <COMMON-NAME>                         | Configures a subject name, defined by the <COMMON-NAME> keyword, to identify the certificate <ul style="list-style-type: none"> <li>• &lt;COMMON-NAME&gt; – Specify the common name used with this certificate. The name should enable you to identify the certificate easily and should not exceed 2 to 64 characters in length.</li> </ul>                                                                                                                            |
| <COUNTRY>                                          | Sets the deployment country code (2 character ISO code)                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <STATE>                                            | Sets the state name (2 to 64 characters in length)                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <CITY>                                             | Sets the city name (2 to 64 characters in length)                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <ORGANIZATION>                                     | Sets the organization name (2 to 64 characters in length)                                                                                                                                                                                                                                                                                                                                                                                                               |
| <ORGANIZATION-UNIT>                                | Sets the organization unit (2 to 64 characters in length)                                                                                                                                                                                                                                                                                                                                                                                                               |

|                       |                                                                                                                                                                                     |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| email <SEND-TO-EMAIL> | Optional. Exports the self-signed certificate to a specified e-mail address <ul style="list-style-type: none"> <li>• &lt;SEND-TO-EMAIL&gt; – Specify the e-mail address.</li> </ul> |
| fqdn <FQDN>           | Optional. Exports the self-signed certificate to a specified FQDN <ul style="list-style-type: none"> <li>• &lt;FQDN&gt; – Specify the FQDN.</li> </ul>                              |
| ip-address <IP>       | Optional. Exports the self-signed certificate to a specified device or system <ul style="list-style-type: none"> <li>• &lt;IP&gt; – Specify the device’s IP address.</li> </ul>     |

```
crypto pki import [certificate|crl] <TRUSTPOINT-NAME> <IMPORT-FROM-URL>
{background} {(on <DEVICE-NAME>)}
```

|                                        |                                                                                                                                                                                                                                                                                                  |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| pki                                    | Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.                                                                                                                                                           |
| import                                 | Imports certificates, Certificate Revocation List (CRL), or a trustpoint to the selected device                                                                                                                                                                                                  |
| [certificate crl]<br><TRUSTPOINT-NAME> | Imports a signed server certificate or CRL <ul style="list-style-type: none"> <li>• certificate – Imports signed server certificate</li> <li>• crl – Imports CRL</li> <li>• &lt;TRUSTPOINT-NAME&gt; – Specify the trustpoint name (should be authenticated).</li> </ul>                          |
| <IMPORT-FROM-URL>                      | Specify the signed server certificate or CRL source address. Both IPv4 and IPv6 address formats are supported.<br>The server certificate or the CRL (based on the parameter passed in the preceding step) is imported from the location specified here.                                          |
| background                             | Optional. Performs import operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the import on.                                                                                                                    |
| on <DEVICE-NAME>                       | The following parameter is recursive and optional: <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; – Optional. Performs import operation on a specified device</li> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
crypto pki import trustpoint <TRUSTPOINT-NAME> <IMPORT-FROM-URL>
{background/passphrase <KEY-PASSPHRASE> background} {(on <DEVICE-NAME>)}
```

|                                 |                                                                                                                                                                                                                                  |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| pki                             | Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.                                                                                           |
| import                          | Imports certificates, CRL, or a trustpoint to the selected device                                                                                                                                                                |
| trustpoint<br><TRUSTPOINT-NAME> | Imports a trustpoint and its associated CA certificate, server certificate, and private key <ul style="list-style-type: none"> <li>• &lt;TRUSTPOINT-NAME&gt; – Specify the trustpoint name (should be authenticated).</li> </ul> |
| <IMPORT-FROM-URL>               | Specify the trustpoint source address. Both IPv4 and IPv6 address formats are supported.                                                                                                                                         |
| background                      | Optional. Performs import operation in the background. If selecting this option, you can optionally specify the device (access point or controller) to perform the import on.                                                    |

|                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| passphrase <KEY-PASSPHRASE><br>background | Optional. Decrypts trustpoint with a passphrase after importing <ul style="list-style-type: none"> <li>• &lt;KEY-PASSPHRASE&gt; – Specify the passphrase. After specifying the passphrase, optionally specify the device to perform import on.</li> <li>• background – Optional. Performs import operation in the background. After specifying the passphrase, optionally specify the device (access point or controller) to perform the import on.</li> </ul> |
| on <DEVICE-NAME>                          | The following parameter is recursive and optional: <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; – Optional. Performs import operation on a specified device</li> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul>                                                                                                                                                               |

```
crypto pki zeroize trustpoint <TRUSTPOINT-NAME> {del-key} {(on <DEVICE-NAME>)}
```

|                                        |                                                                                                                                                                                                                                                                                               |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| pki                                    | Enables PKI management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA certificates.                                                                                                                                                        |
| zeroize trustpoint <TRUSTPOINT-NAME>   | Imports certificates, <i>Certificate Revocation List</i> (CRL), or a trustpoint to the selected device                                                                                                                                                                                        |
| [certificate crl]<br><TRUSTPOINT-NAME> | Deletes a trustpoint and its associated CA certificate, server certificate, and private key <ul style="list-style-type: none"> <li>• &lt;TRUSTPOINT-NAME&gt; – Specify the trustpoint name (should be authenticated).</li> </ul>                                                              |
| del-key                                | Optional. Deletes the private key associated with the server certificate. Optionally specify the device to perform deletion on.                                                                                                                                                               |
| on <DEVICE-NAME>                       | The following parameter is recursive and optional: <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; – Optional. Deletes the trustpoint on a specified device</li> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

### Usage Guidelines

The system supports both IPv4 and IPv6 address formats. Provide source and destination locations using any one of the following options:

- IPv4 URLs:

```
tftp://<hostname|IPv4>[:port]/path/file
```

```
ftp://<user>:<passwd>@<hostname|IPv4>[:port]/path/file
```

```
sftp://<user>@<hostname|IPv4>[:port]/path/file
```

```
http://<hostname|IPv4>[:port]/path/file
```

```
cf:/path/file usb<n>:/path/file
```

- IPv6 URLs:

```
tftp://<hostname|IPv6>[:port]/path/file
```

```
ftp://<user>:<passwd>@<hostname|IPv6>[:port]/path/file
```

```
sftp://<user>@<hostname|IPv6>[:port]/path/file
```

```
http://<hostname|IPv6>[:port]/path/file
```

### Examples (User Exec Mode)

```
rfs4000-229D58>crypto key generate rsa key 1025
RSA Keypair successfully generated
rfs4000-229D58>
rfs4000-229D58>crypto key import rsa test123 url passphrase word background
RSA key import operation is started in background
rfs4000-229D58>
rfs4000-229D58>crypto pki generate self-signed word generate-rsa-key word autogen-subject-
name fqdn word
Successfully generated self-signed certificate
rfs4000-229D58>
rfs4000-229D58>crypto pki zeroize trustpoint word del-key
Successfully removed the trustpoint and associated certificates
%Warning: Applications associated with the trustpoint will start using default-trustpoint
rfs4000-229D58>
rfs4000-229D58>crypto pki authenticate word url background
Import of CA certificate started in background
rfs4000-229D58>
rfs4000-229D58>crypto pki import trustpoint word url passphrase word
Import operation started in background
rfs4000-229D58>
```

### Examples (Privi Exec Mode)

```
NOC-NX9500#crypto key generate rsa key 2048
RSA key size > 2048. Key generation started in background.
NOC-NX9500#c
```

### Related Commands

|                                             |                                                                            |
|---------------------------------------------|----------------------------------------------------------------------------|
| <code>no (user exec mode)</code> on page 83 | Removes server certificates, trustpoints and their associated certificates |
|---------------------------------------------|----------------------------------------------------------------------------|

### *crypto-cmp-cert-policy (user and privi exec modes)*

Triggers a Certificate Management Protocol (CMP) certificate update on a specified device or devices



#### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
crypto-cmp-cert-update <TRUSTPOINT-NAME> {on <DEVICE-NAME>}
```

### Parameters

```
crypto-cmp-cert-update <TRUSTPOINT-NAME> {on <DEVICE-NAME>}
```

```
crypto-cmp-cert-update
<TRUSTPOINT-NAME> on
<DEVICE-NAME>
```

Triggers a CMP certificate update on a specified device or devices

- <TRUSTPOINT-NAME> - Specify the target trustpoint name. A trustpoint represents a CA/identity pair containing the identity of the CA, CA specific configuration parameters, and an association with an enrolled identity certificate. Use the crypto-cmp-policy context mode to configure the trustpoint.
- on <DEVICE-NAME> - Optional. Initiates a CMP certificate update and response on a specified device or devices. Specify the name of the AP, wireless controller, or service platform. Multiple devices can be provided as a comma separated list.  
    <DEVICE-NAME> - Specify the name of the AP, wireless controller, or service platform.

### Example (User Exec Mode)

```
rfs4000-229D58>crypto-cmp-cert-update test on B4-C7-99-71-17-28
CMP Cert update success
rfs4000-229D58>
```

### Example (Privi Exec Mode)

```
NOC-NX9500#crypto-cmp-cert-update test on NOC-NX9500
CMP Cert update success
NOC-NX9500#
```

*database (user and privi exec modes)*

Enables automatic repairing (vacuuming) and dropping of captive-portal and NSight databases

If enforcing authenticated access to the database, use this command to generate the keyfile. Every keyfile has a set of associated users having a username and password. Access to the database is allowed only if the user credentials entered during database login are valid. For more information on enabling database authentication, see [Enabling Database Authentication](#).



#### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

### Supported in the following platforms:

- Service Platforms — NX 95XX, NX 96XX, VX 9000

### Syntax

```
database [drop|keyfile|repair]
database drop [all|captive-portal|nsight]
database repair {on <DEVICE-NAME>}
database keyfile [export|generate|import|zerzoise]
database keyfile generate
database keyfile [export|import] <URL>
database keyfile zerzoise
```

### Parameters

```
database drop [all|captive-portal|nsight]
```

database drop [all|captive-portal|nsight]

Drops (deletes) all or a specified database. Execute the command on the database.

- all – Drops all databases, captive portal and NSight
- captive-portal – Drops the captive-portal database
- nsight – Drops the NSight database

database repair {on <DEVICE-NAME>}

database repair on <DEVICE-NAME>

Enables automatic repairing of all databases. Repairing (vacuuming a database refers to the process of finding and reclaiming space left over from previous DELETE statements. Execute the command on the database host.

- on <DEVICE-NAME> – Optional. Specifies the name of the database host. When specified, databases on the specified host are periodically checked to identify and remove obsolete data documents.
- <DEVICE-NAME> – Specify the name of the access point, wireless controller, or service platform.

**Note:** If no device is specified, the system repairs all databases.

database keyfile generate

database keyfile generate

Enables database keyfile management. This command is part of a set of configurations required to enforce database authentication. Use this command to generate database keyfiles. After generating the keyfile, create the username and password combination required to access the database. For information on creating database users see, [service](#) on page 647. For information on enabling database authentication, see [Enabling Database Authentication](#).

- generate – Generates the keyfile. In case of a replica-set deployment, execute the command on the primary database host. Once generated, export the keyfile to a specified location from where it is imported on to the replica-set hosts.

database keyfile [export|import] <URL>



database keyfile [export|import] <URL>

Enables database keyfile management. This command is part of a set of configurations required to enforce database authentication. Use this command to exchange keyfiles between replica set members.

- export – Exports the keyfile to a specified location on an FTP/SFTP/TFTP server. Execute the command on the database host on which the keyfile has been generated.
- import – Imports the keyfile from a specified location. Execute the command on the replica set members.

The following parameter is common to both of the above keywords:

- <URL> – Specify the location to/from where the keyfile is to be exported/imported. Use one of the following options to specify the keyfile location:

ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file

sftp://<user>:<passwd>@<hostname|IP>[:port]/path/file

tftp://<hostname|IP>[:port]/path/file

database keyfile zerzoise

database keyfile zerzoise

Enables database keyfile management. Use this command to delete keyfiles

- zerzoise – Deletes an existing keyfile.

### Example (User Exec Mode)

```
nx9500-6C8809nx9500-6C8809>database repair on nx9500-6C8809
nx9500-6C8809>
nx9500-6C8809>database keyfile generate
Database keyfile successfully generated
nx9500-6C8809nx9500-6C8809>
nx9500-6C8809>database keyfile zeroize
Database keyfile successfully removed
nx9500-6C8809nx9500-6C8809>
```

### Example (Privl Exec Mode)

```
vx9000-1A1809#database keyfile generate
Database keyfile successfully generated
vx9000-1A1809#
vx9000-1A1809#database keyfile export ftp://1.1.1.111/db-key
Database keyfile successfully exported
vx9000-1A1809#
vx9000-D031F2#database keyfile import ftp://1.1.1.111/db-key
Database keyfile successfully imported
vx9000-D031F2#
```

### Example: Enabling Database Authentication

Follow the steps below to enable database authentication.

- 1 On the primary database host,
  - a Generate the database keyfile.

```
Primary-DB-HOST>database keyfile generate
Database keyfile successfully generated
Primary-DB-HOST>
```
  - b Use the **show > database > keyfile** command to view the generated keyfile.

- c Export the keyfile to an external location. This is required only in case of database replica-set deployment.
- ```
Primary-DB-HOST>database keyfile export ftp://1.1.1.111/db-key
Database keyfile successfully exported
Primary-DB-HOST>
```
- d Create the users that are allowed access to the database.
- ```
Primary-DB-HOST#service database authentication create-user username techpubs
password techPubs@123
Database user [techpubs] created.
Primary-DB-HOST#
```
- e View the database user account created.
- ```
Primary-DB-HOST#show database users
-----
                DATABASE USER
-----
techpubs
-----
Primary-DB-HOST#
```
- 2 On the replica set host, import the keyfile from the location specified in Step 1 c.
- ```
Secondary-DB-HOST#database keyfile import ftp://1.1.1.111/db-key
```
- 3 In the database-policy context, --- (used on the NSight/EGuest database hosts)
- a Enable authentication.
- ```
Primary-DB-HOST(config-database-policy-techpubs)#authentication
```
- b Configure the user accounts created in Step 1 d.
- ```
Primary-DB-HOST(config-database-policy-techpubs)#authentication username techpubs
password S540QFZz9LzSOdX1ZJEqDgAAAy3b7Gty04Z/Ih2ruxn0Ynr
Primary-DB-HOST(config-database-policy-techpubs)#show context
database-policy techpubs
authentication
authentication username techpubs password 2 S540QFZz9LzSOdX1ZJEqDgAAAy3b7Gty04Z/
Ih2ruxn0Ynr
replica-set member nx7500-A02B91 arbiter
replica-set member vx9000-1A1809 priority 1
replica-set member vx9000-D031F2 priority 20
Primary-DB-HOST(config-database-policy-techpubs)#
```
- 4 In the database-client policy context --- (used on the NSight/EGuest server host), Note, this configuration is required only if the NSight/EGuest server and database are hosted on separate hosts.
- a Configure the user credentials created in Step 1 d.
- ```
NOC-Controller(config-database-client-policy-techpubs)#authentication username
techpubs password S540QFZz9LzSOdX1ZJEqDgAAAy3b7Gty04Z/Ih2ruxn0Ynr
```
- b View the configuration.
- ```
NOC-Controller(config-database-client-policy-techpubs)#show context
database-client-policy techpubs
authentication username techpubs password 2 S540QFZz9LzSOdX1ZJEqDgAAAy3b7Gty04Z/
Ih2ruxn0Ynr
NOC-Controller(config-database-client-policy-techpubs)#
```

## Related Commands

|                                                                         |                                                                                                          |
|-------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| <a href="#">database-backup (user and privi exec modes)</a> on page 63  | Backs up captive-portal and/or NSight database to a specified location and file on an FTP or SFTP server |
| <a href="#">database-restore (user and privi exec modes)</a> on page 64 | Restores a previously exported database [captive-portal and/or NSight]                                   |

|                                                                  |                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">database-policy global config</a> on page 363        | Documents database-policy configuration commands. Use this option to enable the database.                                                                                                                                                                                                                                  |
| <a href="#">database-client-policy global-config</a> on page 359 | Documents database-client-policy configuration commands. Use this option to configure the database host details (IP address or hostname). If enforcing database authentication, use it to configure the users having database access. Once configured, use the policy in the NSight/EGuest server's device config context. |
| <a href="#">service</a> on page 647                              | Documents the database user account configuration details                                                                                                                                                                                                                                                                  |

### database-backup (user and privi exec modes)

Backs up captive-portal and/or NSight database to a specified location and file on an FTP, SFTP, or TFTP server. Execute this command on the database host.



#### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

### Supported in the following platforms:

- Service Platforms — NX 95XX, NX 96XX, VX 9000

### Syntax

```
database-backup database [captive-portal|nsight|nsight-placement-info] <URL>
database-backup database [captive-portal|nsight] <URL>
database-backup database nsight-placement-info <URL>
```

### Parameters

```
database-backup database [captive-portal|nsight] <URL>
```

|                                                  |                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| database-backup database [captive-portal nsight] | Backs up captive portal and/or NSight database to a specified location. Select the database to backup: <ul style="list-style-type: none"> <li>• captive-portal - Backs up captive portal database</li> <li>• nsight - Backs up NSight database After specifying the database type, configure the destination location.</li> </ul> |
| <URL>                                            | Configures the destination location. The database is backed up at the specified location. Specify the location URL in one of the following formats:<br>ftp://<user>:<passwd>@<hostname IP>[:port]/path/file.tar.gz<br>sftp://<user>:<passwd>@<hostname IP>[:port]/path/file.tar.gz                                                |

```
database-backup database nsight-placement-info <URL>
```

|                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| database-backup database nsight-placement-info <URL> | Backs up the NSight access point placement related details to a specified location <ul style="list-style-type: none"> <li>• &lt;URL&gt; - Specify the URL in one of the following formats:<br/> ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IP&gt;[:port]/path/file.tar.gz<br/> sftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IP&gt;[:port]/path/file.tar.gz<br/> tftp://&lt;hostname IP&gt;[:port]/path/file.tar.gz</li> </ul> |
|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Example (User Exec Mode)

```
NS-DB-nx9510-6C87EF>database-backup database nsight tftp://192.168.9.50/testbckup
NS-DB-nx9510-6C87EF>show database backup-status
Last Database Backup Status : In_Progress(Starting tftp transfer.)
Last Database Backup Time : 2018-01-01 12:48:05
NS-DB-nx9510-6C87EF>show database backup-status
Last Database Backup Status : Successful
Last Database Backup Time : Mon Jan 01 12:48:08 IST 2018
NS-DB-nx9510-6C87EF>
```

### Example (Privi Exec Mode)

```
NS-DB-nx9510-6C87EF#database-backup database nsight-placement-info tftp://192.168.9.50/
plmentinfo
NS-DB-nx9510-6C87EF#show database backup-status
Last Database Backup Status : Successful
Last Database Backup Time : Mon Jan 01 12:48:48 IST 2018
NS-DB-nx9510-6C87EF#
```

### Related Commands

|                                                                         |                                                                                                  |
|-------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| <a href="#">database (user and privi exec modes)</a> on page 59         | Enables automatic repairing (vacuuming) and dropping of databases (captive-portal and/or NSight) |
| <a href="#">database-restore (user and privi exec modes)</a> on page 64 | Restores a previously exported (backed up) database (captive-portal and/or NSight)]              |

### *database-restore (user and privi exec modes)*

Restores a previously exported database [captive-portal and/or NSight]. Previously exported databases (backed up to a specified FTP or SFTP server) are restored from the backed-up location to the original database.



#### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

### Supported in the following platforms:

- Service Platforms — NX 95XX, NX 96XX, VX 9000

### Syntax

```
database-restore database [captive-portal|nsight] <URL>
```

### Parameters

```
database-restore database [captive-portal|nsight] <URL>
```

|                                                    |                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| database-restore database [captive-portal  nsight] | Restores previously exported (backed up) captive-portal and/or NSight database. Specify the database type: <ul style="list-style-type: none"> <li>• captive-portal – Restores captive portal database</li> <li>• nsight – Restores NSight database</li> </ul> After specifying the database type, configure the destination location and file name from where the files are restored. |
| <URL>                                              | Configures the destination location. The database is restored from the specified location. Specify the location URL in one of the following formats:<br>ftp://<user>:<passwd>@<hostname IP>[:port]/path/file.tar.gz<br>sftp://<user>:<passwd>@<hostname IP>[:port]/path/file.tar.gz<br>tftp://<hostname IP>[:port]/path/file.tar.gz                                                   |

### Example (User Exec Mode)

```
nx9500-6C8809>database-restore database nsight ftp://anonymous:anonymous@192.168.13.10/backups/nsight/nsight.tar.gz
```

### Example (Privi Exec Mode)

```
nx9500-6C874D#database-restore database nsight ftp://anonymous:anonymous@192.168.13.10/backups/nsight/nsight.tar.gz
```

### Related Commands

|                                                        |                                                                                                          |
|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| database (user and privi exec modes) on page 59        | Enables automatic repairing (vacuuming) and dropping of databases (captive-portal and NSight)            |
| database-backup (user and privi exec modes) on page 63 | Backs up captive-portal and/or NSight database to a specified location and file on an FTP or SFTP server |

### *device-upgrade (user and privi exec modes)*

Enables firmware upgrade on an adopted device or a set of adopted devices (Access Points, wireless controllers, and service platforms)



#### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

In an HM (hierarchically managed) network, this command enables centralized device upgradation across the network.

The WiNG HM network defines a three-tier structure, consisting of multiple wireless sites managed by a single NOC (Network Operations Center) controller. The NOC controller constitutes the first and the site controllers constitute the second tier of the hierarchy respectively. The site controllers may or may not be grouped to form clusters. The site controllers in turn adopt and manage access points that form the third tier of the hierarchy.



#### Note

Hierarchical management allows the NOC controller to upgrade controllers and access points that are directly or indirectly adopted to it. However, ensure that the NOC controller is loaded with the correct firmware version.

Use the device-upgrade command to schedule firmware upgrades across adopted devices within the network. Devices are upgraded based on their device names, MAC addresses, or RF Domain.



#### Note

If the persist-images option is selected, the RF Domain manager retains the old firmware image, or else deletes it. For more information on enabling device upgrade on profiles and devices (including the 'persist-images' option), see [device-upgrade](#) on page 981.



#### Note

A NOC controller's capacity is equal to, or higher than that of a site controller. The following devices can be deployed at NOC and sites:

- NOC controller – NX 95XX, NX 96XX, VX 9000
- Site controller – RFS 4000, NX 5500, or NX 75XX



#### Note

Standalone devices have to be manually upgraded.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000, RFS 6000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
device-upgrade [<MAC/HOSTNAME>|all|ap6522|ap6562|ap7161|ap7502|ap7522|ap7532|ap7602|
ap7612|ap7622|ap7632|ap7662|ap8163|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx9000|nx9600|
vx9000|cancel-upgrade|load-image|rf-domain]
device-upgrade <MAC/HOSTNAME> {no-reboot|reboot-time <TIME>/upgrade-time <TIME>
{no-reboot|reboot-time <TIME>}}
device-upgrade all {no-reboot|reboot-time <TIME>/upgrade-time <TIME>
{no-reboot|reboot-time <TIME>}} {(staggered-reboot)}
device-upgrade [ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|
ap7632|ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx9000|nx9600|vx9000] all
{force|no-reboot|reboot-time <TIME>/upgrade-time <TIME> {no-reboot|reboot-time <TIME>}}
{(staggered-reboot)}
device-upgrade cancel-upgrade [<MAC/HOSTNAME>|all|ap6522|ap6562|ap71xx|ap7502|ap7522|
ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|
nx75xx|nx9000|nx9600|vx9000|on rf-domain [<RF-DOMAIN-NAME>|all]]
device-upgrade load-image [ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|
ap7612|ap7622|ap7632|ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx9000|nx9600|vx9000]
{<IMAGE-URL>|on <DEVICE-OR-DOMAIN-NAME>}
device-upgrade rf-domain [<RF-DOMAIN-NAME>|all|containing <WORD>|filter location <WORD>]
[all|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap76232|
ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx9000|nx9600|vx9000]
{(<MAC/HOSTNAME>|force|from-controller|no-reboot|reboot-time <TIME>/staggered-reboot|
upgrade-time <TIME>)}
```

### Parameters

```
device-upgrade <MAC/HOSTNAME> {no-reboot|reboot-time <TIME>/upgrade-time <TIME>
{no-reboot|reboot-time <TIME>}}
```

|                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <MAC/HOSTNAME>                                      | Upgrades firmware on the device identified by the <MAC/HOSTNAME> keyword <ul style="list-style-type: none"> <li>• &lt;MAC/HOSTNAME&gt; - Specify the device's MAC address or hostname.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                  |
| no-reboot                                           | Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| reboot-time <TIME>                                  | Optional. Schedules an automatic reboot after a successful upgrade <ul style="list-style-type: none"> <li>• &lt;TIME&gt; - Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                             |
| upgrade-time <TIME> {no-reboot  reboot-time <TIME>} | Optional. Schedules an automatic device firmware upgrade <ul style="list-style-type: none"> <li>• &lt;TIME&gt; - Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format. The following actions can be performed after a scheduled upgrade: <ul style="list-style-type: none"> <li>• no-reboot - Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)</li> <li>• reboot-time &lt;TIME&gt; - Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.</li> </ul> </li> </ul> |

```
device-upgrade all {force/no-reboot/reboot-time <TIME>/upgrade-time <TIME>
{no-reboot/reboot-time <TIME>}} {(staggered-reboot)}
```

|                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| all                                                 | Upgrades firmware on all devices                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| force                                               | Optional. Select this option to force upgrade on the selected device(s). When selected, the devices are upgraded even if they have the same firmware as the upgrading access point, wireless controller, or service platform. If forcing a device upgrade, optionally specify any one of the following options: no-reboot, reboot-time, upgrade-time, or staggered-reboot.                                                                                                                                                                                                                                                                                                     |
| no-reboot                                           | Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| reboot-time <TIME>                                  | Optional. Schedules an automatic reboot after a successful upgrade <ul style="list-style-type: none"> <li>• &lt;TIME&gt; - Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| upgrade-time <TIME> {no-reboot  reboot-time <TIME>} | Optional. Schedules an automatic firmware upgrade on all devices, of the specified type, on a specified day and time <ul style="list-style-type: none"> <li>• &lt;TIME&gt; - Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format. The following actions can be performed after a scheduled upgrade: <ul style="list-style-type: none"> <li>• no-reboot - Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)</li> <li>• reboot-time &lt;TIME&gt; - Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.</li> </ul> </li> </ul> |
| staggered-reboot                                    | This keyword is recursive and common to all of the above. <ul style="list-style-type: none"> <li>• Optional. Enables staggered reboot (one at a time), without network impact</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

```
device-upgrade [ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|
ap7622|ap7632|ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx9000|nx9600|vx9000]
all {force/no-reboot/reboot-time <TIME>/upgrade-time <TIME>
{no-reboot/reboot-time <TIME>}} {(staggered-reboot)}
```

|                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| device-upgrade<br><DEVICE-TYPE><br>all                | Upgrades firmware on all devices of a specific type. Select the device type. The options are: AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533, RFS 4000, NX 5500, NX 75XX, NX 95XX, NX 96XX, and VX 9000.<br>After selecting the device type, schedule an automatic upgrade and/or an automatic reboot.                                                                                                                                                                                                                                                                                           |
| force                                                 | Optional. Select this option to force upgrade on the selected device(s). When selected, the devices are upgraded even if they have the same firmware as the upgrading access point, wireless controller, or service platform. If forcing a device upgrade, optionally specify any one of the following options: no-reboot, reboot-time, upgrade-time, or staggered-reboot.                                                                                                                                                                                                                                                                                                     |
| no-reboot                                             | Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| reboot-time<br><TIME>                                 | Optional. Schedules an automatic reboot after a successful upgrade <ul style="list-style-type: none"> <li>• &lt;TIME&gt; – Optional. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| upgrade-time<br><TIME> {no-reboot reboot-time <TIME>} | Optional. Schedules an automatic firmware upgrade on all devices, of the specified type, on a specified day and time <ul style="list-style-type: none"> <li>• &lt;TIME&gt; – Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format. The following actions can be performed after a scheduled upgrade: <ul style="list-style-type: none"> <li>• no-reboot – Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)</li> <li>• reboot-time &lt;TIME&gt; – Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.</li> </ul> </li> </ul> |
| staggered-reboot                                      | This keyword is recursive and common to all of the above. <ul style="list-style-type: none"> <li>• Optional. Enables staggered reboot (one at a time), without network impact</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

```
device-upgrade cancel-upgrade [<MAC/HOSTNAME>|all|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx9000|nx9600|vx9000|on rf-domain [<RF-DOMAIN-NAME>|all]]
```

|                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cancel-upgrade                             | Cancels a scheduled firmware upgrade based on the parameters passed. This command provides the following options to cancel scheduled firmware upgrades: <ul style="list-style-type: none"> <li>• Cancels upgrade on specific device(s). The devices are identified by their MAC addresses or hostnames.</li> <li>• Cancels upgrade on all devices within the network</li> <li>• Cancels upgrade on all devices of a specific type. Specify the device type.</li> <li>• Cancels upgrade on specific device(s) or all device(s) within a specific RF Domain or all RF Domains. Specify the RF Domain name.</li> </ul> |
| cancel-upgrade<br>[<MAC/<br>HOSTNAME> all] | Cancels a scheduled firmware upgrade on a specified device or on all devices <ul style="list-style-type: none"> <li>• &lt;MAC/HOSTNAME&gt; – Cancels a scheduled upgrade on the device identified by the &lt;MAC/HOSTNAME&gt; keyword. Specify the device's MAC address or hostname.</li> <li>• all – Cancels scheduled upgrade on all devices</li> </ul>                                                                                                                                                                                                                                                           |



|                                                           |                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cancel-upgrade<br><DEVICE-TYPE> all                       | Cancels scheduled firmware upgrade on all devices of a specific type. Select the device type. The options are: AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533, RFS 4000, NX 5500, NX 75XX, NX 95XX, NX 96XX, and VX 9000.                                                                |
| cancel-upgrade on<br>rf-domain [<RF-<br>DOMAIN-NAME> all] | Cancels scheduled firmware upgrade on all devices in a specified RF Domain or all RF Domains <ul style="list-style-type: none"> <li>• &lt;RF-DOMAIN-NAME&gt; - Cancels scheduled device upgrade on all devices in a specified RF Domain. Specify the RF Domain name.</li> <li>• all - Cancels scheduled device upgrade on all devices across all RF Domains</li> </ul> |

```
device-upgrade load-image [ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|
ap7612|ap7622|ap7632|ap7662|ap81xx|ap8432|ap8533|rfs4000|nx500|nx9000|nx9600|vx9000]
{<IMAGE-URL>|on <DEVICE-OR-DOMAIN-NAME>}
```

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| load-image <DEVICE-TYPE>       | Loads device firmware image from a specified location. Use this command to specify the device type and the location of the corresponding image file. <ul style="list-style-type: none"> <li>• &lt;DEVICE-TYPE&gt; - Specify the device type. The options are: AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533, RFS 4000, NX 5500, NX 75XX, NX 95XX, NX 96XX, and VX 9000.</li> </ul> <p>After specifying the device type, provide the location of the required device firmware image.</p>                                                                                                                                                                                                                                                             |
| <IMAGE-URL>                    | Specify the device's firmware image location in one of the following formats:<br>IPv4 URLs: <ul style="list-style-type: none"> <li>• tftp://&lt;hostname IP&gt;[:port]/path/file</li> <li>• ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IP&gt;[:port]/path/file</li> <li>• sftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IP&gt;[:port]/path/file</li> <li>• http://&lt;hostname IP&gt;[:port]/path/file</li> <li>• cf:/path/file</li> <li>• usb&lt;n&gt;:/path/file</li> </ul> IPv6 URLs: <ul style="list-style-type: none"> <li>• tftp://&lt;hostname IPv6&gt;[:port]/path/file</li> <li>• ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IPv6&gt;[:port]/path/file</li> <li>• sftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IPv6&gt;[:port]/path/file</li> <li>• http://&lt;hostname IPv6&gt;[:port]/path/file</li> </ul> |
| on <DEVICE-OR-DOMAIN-<br>NAME> | Specify the name of the device or RF Domain. The image, of the specified device type is loaded from the device specified here. In case of an RF Domain, the image available on the RF Domain manager is loaded. <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; - Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                               |

```
device-upgrade rf-domain [<RF-DOMAIN-NAME>|all|containing <WORD>|
filter location <WORD>] [all|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|
ap7612|ap7622|ap7632|ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx9000|nx9600|
vx9000] {(<MAC/HOSTNAME>|force|from-controller|no-reboot|reboot-time <TIME>|
staggered-reboot|upgrade-time <TIME>)}
```

|                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| rf-domain [<RF-DOMAIN-NAME>  all  containing <WORD>  filter location <WORD>] | <p>Upgrades firmware on devices in a specified RF Domain or all RF Domains. Devices within a RF Domain are upgraded through the RF Domain manager.</p> <ul style="list-style-type: none"> <li>• &lt;RF-DOMAIN-NAME&gt; - Upgrades devices in the RF Domain identified by the &lt;RF-DOMAIN-NAME&gt; keyword.</li> <li>• &lt;RF-DOMAIN-NAME&gt; - Specify the RF Domain name.</li> <li>• all - Upgrades devices across all RF Domains</li> <li>• containing &lt;WORD&gt; - Filters RF Domains by their names. RF Domains with names containing the sub-string identified by the &lt;WORD&gt; keyword are filtered. Devices on the filtered RF Domains are upgraded.</li> <li>• filter location &lt;WORD&gt; - Filters devices by their location. All devices with location matching the &lt;WORD&gt; keyword are upgraded.</li> </ul> |
| <DEVICE-TYPE>                                                                | <p>After specifying the RF Domain, select the device type. The options are: AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533, RFS 4000, NX 5500, NX 75XX, NX 95XX, NX 96XX, and VX 9000. After specifying the RF Domain and the device type, configure any one of the following actions: force devices to upgrade, or initiate an upgrade through the adopting controller.</p>                                                                                                                                                                                                                                                                                                                                                                           |
| <MAC/HOSTNAME>                                                               | <p>Optional. Use this option to identify specific devices for upgradation. Specify the device's MAC address or hostname. The device should be within the specified RF Domain and of the specified device type. After identifying the devices to upgrade, configure any one of the following actions: force devices to upgrade, or initiate an upgrade through the adopting controller.</p> <p><b>Note:</b> If no MAC address or hostname is specified, all devices of the type selected are upgraded.</p>                                                                                                                                                                                                                                                                                                                            |
| force                                                                        | <p>Optional. Select this option to force upgrade for the selected device(s). When selected, the devices are upgraded even if they have the same firmware as the upgrading access point, wireless controller, or service platform. If forcing a device upgrade, optionally specify any one of the following options: no-reboot, reboot-time, upgrade-time, or reboot-time.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| from-controller                                                              | <p>Optional. Upgrades a device through the adopted device. If initiating an upgrade through the adopting controller, optionally specify any one of the following options: no-reboot, reboot-time, upgrade-time, or reboot-time.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| no-reboot {staggered-reboot}                                                 | <p>Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| reboot-time <TIME> {staggered-reboot}                                        | <p>Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| staggered-reboot                                                             | <p>This keyword is common to all of the above. Optional. Enables staggered reboot (one at a time) without network impact</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| upgrade-time <TIME> {no-reboot  reboot-time <TIME>}                          | <p>Optional. Schedules an automatic firmware upgrade</p> <ul style="list-style-type: none"> <li>• &lt;TIME&gt; - Specify the upgrade time in the MM/DD/YYYY-HH:MM or HH:MM format. After a scheduled upgrade, the following actions can be performed. <ul style="list-style-type: none"> <li>• no-reboot - Optional. Disables automatic reboot after a successful upgrade the device must be manually restarted)</li> <li>• reboot-time &lt;TIME&gt; - Optional. Schedules an automatic reboot after a successful upgrade. Specify the reboot time in the MM/DD/YYYY-HH:MM or HH:MM format.</li> </ul> </li> </ul>                                                                                                                                                                                                                   |

### Example (User Exec Mode)

```
NOC-NX9500>show adoption status
```

```


```

| DEVICE-NAME<br>UPTIME     | VERSION      | CFG-STAT         | SGS | ADOPTED-BY | LAST-ADOPTION    |
|---------------------------|--------------|------------------|-----|------------|------------------|
| nx7500-3D1F06<br>22:32:38 | 5.9.2.0-004D | version-mismatch | No  | NOC-NX9500 | 2 days 12:23:52  |
| t5-ED7C6C<br>22:33:25     | 5.4.2.0-010R | configured       | No  | NOC-NX9500 | 13 days 22:47:46 |

-----  
 Total number of devices displayed: 2  
 NOC-NX9500>  
 NOC-NX9500>show device-upgrade versions

| CONTROLLER        | DEVICE-TYPE   | VERSION      |
|-------------------|---------------|--------------|
| NOC-NX9500        | ap621         | none         |
| NOC-NX9500        | ap622         | 5.9.2.0-005D |
| NOC-NX9500        | ap650         | none         |
| NOC-NX9500        | ap6511        | none         |
| NOC-NX9500        | ap6521        | none         |
| NOC-NX9500        | ap6522        | 5.9.2.0-005D |
| NOC-NX9500        | ap6532        | none         |
| NOC-NX9500        | ap6562        | 5.9.2.0-005D |
| NOC-NX9500        | ap71xx        | 5.9.2.0-005D |
| NOC-NX9500        | ap7502        | 5.9.2.0-005D |
| NOC-NX9500        | ap7522        | 5.9.2.0-005D |
| NOC-NX9500        | ap7532        | 5.9.2.0-005D |
| NOC-NX9500        | ap7562        | 5.9.2.0-005D |
| NOC-NX9500        | ap7602        | 5.9.2.0-005D |
| NOC-NX9500        | ap7612        | 5.9.2.0-005D |
| NOC-NX9500        | ap7622        | 5.9.2.0-005D |
| NOC-NX9500        | ap7632        | 5.9.2.0-005D |
| NOC-NX9500        | ap7662        | 5.9.2.0-005D |
| NOC-NX9500        | ap81xx        | 5.9.2.0-005D |
| NOC-NX9500        | ap82xx        | none         |
| NOC-NX9500        | ap8432        | 5.9.2.0-005D |
| NOC-NX9500        | ap8533        | 5.9.2.0-005D |
| NOC-NX9500        | nx45xx        | none         |
| NOC-NX9500        | nx5500        | none         |
| NOC-NX9500        | nx65xx        | none         |
| <b>NOC-NX9500</b> | <b>nx75xx</b> | <b>none</b>  |
| NOC-NX9500        | nx9000        | none         |
| NOC-NX9500        | rfs4000       | 5.9.2.0-005D |
| NOC-NX9500        | rfs6000       | none         |
| NOC-NX9500        | rfs7000       | none         |
| NOC-NX9500        | vx9000        | none         |

NOC-NX9500>  
 NOC-NX9500#**device-upgrade load-image nx75xx**  
**ftp://anonymous:anonymous@192.168.13.10/LatestBuilds/W592/NX7500-LEAN-5.9.0.2-005D**

| ONTROLLER  | STATUS  | MESSAGE                           |
|------------|---------|-----------------------------------|
| NOC-NX9500 | Success | Successfully initiated load image |

NOC-NX9500#  
 NOC-NX9500#show device-upgrade load-image-status  
 Download of nx7500 firmware file is complete  
 NOC-NX9500#  
 NOC-NX9500>show device-upgrade versions

| CONTROLLER | DEVICE-TYPE | VERSION |
|------------|-------------|---------|
|------------|-------------|---------|

```

NOC-NX9500 ap621 none
NOC-NX9500 ap622 5.9.2.0-005D
NOC-NX9500 ap650 none
NOC-NX9500 ap6511 none
NOC-NX9500 ap6521 none
NOC-NX9500 ap6522 5.9.2.0-005D
NOC-NX9500 ap6532 none
NOC-NX9500 ap6562 5.9.2.0-005D
NOC-NX9500 ap71xx 5.9.2.0-005D
NOC-NX9500 ap7502 5.9.2.0-005D
NOC-NX9500 ap7522 5.9.2.0-005D
NOC-NX9500 ap7532 5.9.2.0-005D
NOC-NX9500 ap7562 5.9.2.0-005D
NOC-NX9500 ap7602 5.9.2.0-005D
NOC-NX9500 ap7612 5.9.2.0-005D
NOC-NX9500 ap7622 5.9.2.0-005D
NOC-NX9500 ap7632 5.9.2.0-005D
NOC-NX9500 ap7662 5.9.2.0-005D
NOC-NX9500 ap81xx 5.9.2.0-005D
NOC-NX9500 ap82xx none
NOC-NX9500 ap8432 5.9.2.0-005D
NOC-NX9500 ap8533 5.9.2.0-005D
NOC-NX9500 nx45xx none
NOC-NX9500 nx5500 none
NOC-NX9500 nx65xx none
NOC-NX9500 nx75xx 5.9.2.0-005D
NOC-NX9500 nx9000 none
NOC-NX9500 rfs4000 5.9.2.0-005D
NOC-NX9500 rfs6000 none
NOC-NX9500 rfs7000 none
NOC-NX9500 vx9000 none

```

```

NOC-NX9500>
NOC-NX9500>device-upgrade nx7500-3D1F06

```

| CONTROLLER        | STATUS  | MESSAGE                     |
|-------------------|---------|-----------------------------|
| B4-C7-99-6C-88-09 | Success | Queued 1 devices to upgrade |

```

NOC-NX9500>
NOC-NX9500>show device-upgrade status
Number of devices currently being upgraded : 1
Number of devices waiting in queue to be upgraded : 0
Number of devices currently being rebooted : 0
Number of devices waiting in queue to be rebooted : 0
Number of devices failed upgrade : 0

```

| DEVICE        | STATE       | UPGRADE TIME | REBOOT TIME | PROGRESS | RETRIES | LAST UPDATE |
|---------------|-------------|--------------|-------------|----------|---------|-------------|
| nx7500-3D1F06 | downloading | immediate    | immediate   | 17       | 0       | -           |

```

NOC-NX9500>

```

### Example (Privi Exec Mode)

```

nx9500-6C874D#device-upgrade rfs4000-229D58

```

| CONTROLLER | STATUS | MESSAGE |
|------------|--------|---------|
|------------|--------|---------|

```

B4-C7-99-6C-87-4D Success Queued 1 devices to upgrade

nx9500-6C874D#show device-upgrade status
Number of devices currently being upgraded : 0
Number of devices waiting in queue to be upgraded : 1
Number of devices currently being rebooted : 0
Number of devices waiting in queue to be rebooted : 0
Number of devices failed upgrade : 0

 DEVICE STATE UPGRADE TIME REBOOT TIME PROGRESS RETRIES LAST UPDATE ERROR
UPGRADED BY

 rfs4000-229D58 waiting immediate immediate 0 0 -
nx9500-6C874D

nx9500-6C874D#

```

## delete

Deletes a specified file from the device's file system

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
delete [/force <FILE>|/recursive <FILE>|<FILE>]
```

### Parameters

```
delete [/force <FILE>|/recursive <FILE>|<FILE>]
```

|            |                                                                                                                                      |
|------------|--------------------------------------------------------------------------------------------------------------------------------------|
| /force     | Forces deletion without a prompt                                                                                                     |
| /recursive | Performs a recursive delete                                                                                                          |
| <FILE>     | Specifies the file name <ul style="list-style-type: none"> <li>• Deletes the file specified by the &lt;FILE&gt; parameter</li> </ul> |

### Examples

```

rfs4000-229D58#delete flash:/out.tar flash:/out.tar.gz
Delete flash:/out.tar [y/n]? y
Delete flash:/out.tar.gz [y/n]? y
rfs4000-229D58
rfs4000-229D58#delete /force flash:/tmp.txt
rfs4000-229D58#
rfs4000-229D58#delete /recursive flash:/backup/
Delete flash:/backup//fileMgmt_350_180B.core
[y/n]? y
Delete flash:/backup//fileMgmt_350_18212X.core_bk
[y/n]? n
Delete flash:/backup//imish_1087_18381X.core.gz

```

```
[y/n]? n
rfs4000-229D58
```

## *diff*

Displays the differences between two files on a device's file system or a particular URL

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
diff [<FILE>|<URL>] [<FILE>|<URL>]
```

### Parameters

```
diff [<FILE>|<URL>] [<FILE>|<URL>]
```

|                                                                                                            |
|------------------------------------------------------------------------------------------------------------|
| <FILE> The first <FILE> is the source file for the diff command. The second <FILE> is used for comparison. |
| <URL> The first <URL> is the source file's URL. The second <URL> is the second file's URL.                 |

### Examples

```
nx9500-6C8809#diff startup-config running-config
--- startup-config
+++ running-config
@@ -1,12 +1,10 @@
+!### show running-config
!
! Configuration of NX9500 version 5.9.2.0-012D
!
!
version 2.5
!
-password-encryption-version 1.0
-inline-password-encryption
-password-encryption-key secret 2
776f9d6d5bb08fac753394d779cbc5a200000020a4ca26def55d4d77952308cd5e3afc66c06581bb1e5af6d6b03
3fd664c363522
!
client-identity-group default
load default-fingerprints
@@ -35,13 +33,13 @@
!
alias string $IN-Blr-EcoSpace-Floor-4 IBEF4
!
-alias encrypted-string $READ 2 LKSXiTieTV5hybKxfgbd6JwAAAAZ/lakoqHh/ZfyHLJWzluTH
+alias encrypted-string $READ 2 log6ZeMyEVJhybKxfgbd6JwAAAAahnGq6RaJb70CEIbVpTYre
--More--
nx9500-6C8809#
```

## *dir*

Lists files on a device's file system

## Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
dir {/all//recursive|<DIR>|all-filestems}
```

## Parameters

```
dir {/all//recursive|<DIR>|all-filestems}
```

|               |                                              |
|---------------|----------------------------------------------|
| /all          | Optional. Lists all files                    |
| /recursive    | Optional. Lists files recursively            |
| <DIR>         | Optional. Lists files in the named file path |
| all-filestems | Optional. Lists files on all file systems    |

## Examples

```
nx9500-6C8809#dir flash:/
```

```
Directory of flash:/
```

```
-rw- 62937 Tue Nov 24 16:00:06 2015 run-config-backup.txt
drwx Tue Nov 29 09:48:42 2016 crashinfo
drwx Sat Sep 17 05:14:43 2016 upgrade
drwx Mon Sep 28 09:48:33 2015 tmptpd
drwx Wed Feb 15 11:53:07 2017 log
drwx Wed Feb 15 11:02:55 2017 archived_logs
drwx Tue May 24 22:23:54 2016 cache
drwx Thu Feb 19 08:53:45 2015 floorplans
-rw- 42018304 Tue Sep 27 10:19:24 2016 in.tar
drwx Tue Jan 17 10:02:01 2017 hotspot
```

```
nx9500-6C8809#
```

```
nx9500-6C8809#dir all-filestems
```

```
Directory of flash:/
```

```
-rw- 62937 Tue Nov 24 16:00:06 2015 run-config-backup.txt
drwx Tue Nov 29 09:48:42 2016 crashinfo
drwx Sat Sep 17 05:14:43 2016 upgrade
drwx Mon Sep 28 09:48:33 2015 tmptpd
drwx Wed Feb 15 11:53:07 2017 log
drwx Wed Feb 15 11:02:55 2017 archived_logs
drwx Tue May 24 22:23:54 2016 cache
drwx Thu Feb 19 08:53:45 2015 floorplans
-rw- 42018304 Tue Sep 27 10:19:24 2016 in.tar
drwx Tue Jan 17 10:02:01 2017 hotspot
```

```
Directory of nvram:/
```

```
lrwx 29 Tue Oct 27 16:22:21 2015 sensor_default_scan
```

```
--More--
```

```
nx9500-6C8809#
```

## *disable*

Turns off (disables) the privileged mode command set. This command returns to the User Executable mode.

### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### **Syntax**

```
disable
```

### **Parameters**

None

### **Examples**

```
nx9500-6C8809#disable
nx9500-6C8809>
```

## *edit*

Edits a text file on the device's file system

### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### **Syntax**

```
edit <FILE>
```

### **Parameters**

```
edit <FILE>
```

|        |                                         |
|--------|-----------------------------------------|
| <FILE> | Specify the name of the file to modify. |
|--------|-----------------------------------------|

### **Examples**

```
nx9500-6C8809#edit startup-config
GNU nano 1.2.4 File: startup-config

!
! Configuration of NX9500 version 5.9.2.0-029R
!
!
version 2.5
!
!
client-identity-group default
load default-fingerprints
```



```

!
ip access-list BROADCAST-MULTICAST-CONTROL
 permit tcp any any rule-precedence 10 rule-description "permit all TCP traffic"
 permit udp any eq 67 any eq dhcp rule-precedence 11 rule-description "permit $
 deny udp any range 137 138 any range 137 138 rule-precedence 20 rule-descripti$
 deny ip any 224.0.0.0/4 rule-precedence 21 rule-description "deny IP multicast"
 deny ip any host 255.255.255.255 rule-precedence 22 rule-description "deny IP $
 permit ip any any rule-precedence 100 rule-description "permit all IP traffic"
!
mac access-list PERMIT-ARP-AND-IPv4
 [Read 106 lines]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Txt ^T To Spell

```

## enable

Turns on (enables) the privileged mode command set. This command does not do anything in the Privilege Executable mode.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
enable
```

### Parameters

None

### Examples

```

nx9500-6C8809#enable
nx9500-6C8809#

```

## erase

Erases a device's (wireless controller, Access Point, and service platform) file system. Erases the content of the specified storage device. Also erases the startup configuration to restore the device to its default.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```

erase [flash:|nvram:|startup-config|usb1:|usb2:|usb3:|usb4:]
erase [flash:|nvram:|usb1:|usb2:|usb3:|usb4:]
erase startup-config {<HOSTNAME/MAC>|on <DOMAIN-NAME> {containing <SUB-STRING>|
exclude-controllers|exclude-rf-domain-manager|filter <DEVICE-TYPE>}}

```

## Parameters

erase [flash:|nvram:|usb1:|usb2:|usb3:|usb4:]

|                |                                                                                                                                 |
|----------------|---------------------------------------------------------------------------------------------------------------------------------|
| flash:         | Erases everything in the device's flash: file                                                                                   |
| nvram:         | Erases everything in the device's nvram: file                                                                                   |
| startup-config | Erases the device's startup configuration file. The startup configuration file is used to configure the device when it reboots. |
| usb1:          | Erases everything in the device's usb1: file                                                                                    |
| usb2:          | Erases everything in the device's usb2: file                                                                                    |
| usb3:          | Erases everything in the device's usb3: file                                                                                    |
| usb4:          | Erases everything in the device's usb4: file                                                                                    |

erase startup-config {<HOSTNAME/MAC>|on <DOMAIN-NAME> {containing <SUB-STRING>|exclude-controllers|exclude-rf-domain-manager|filter <DEVICE-TYPE>}}

|                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| startup-config:                                                                                               | Erases the startup configuration file on a specified device or devices in a specified RF Domain. The specified device(s) are reloaded after the startup configuration file is erased. Use the <b>&lt;HOSTNAME/MAC&gt;</b> or <b>on &lt;DOMAIN-NAME&gt;</b> options to identify the device or RF Domain respectively. Once executed, the configuration file, for the targeted device or for all device(s) in the targeted RF Domain, is also erased from the adopting controller's configuration file. They are automatically reloaded once the startup configuration file has been erased.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <HOSTNAME/MAC>                                                                                                | Optional. Erases the startup configuration file on the device identified by the <HOSTNAME/MAC> keyword. Specify the device's hostname or MAC address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| on <DOMAIN-NAME> {containing <SUB-STRING> exclude-controllers exclude-rf-domain-manager filter <DEVICE-TYPE>} | <p>Optional. Erases the startup configuration file on all devices or specified device(s) in a specified RF Domain</p> <ul style="list-style-type: none"> <li>• &lt;DOMAIN-NAME&gt; - Specify the RF Domain name. After specifying the RF Domain, optionally use the filters provided to identify specific device(s) within the RF Domain. If none of the filters are used, the command is executed on all devices within the RF Domain. These filters are: <ul style="list-style-type: none"> <li>• containing &lt;SUB-STRING&gt; - Optional. Executes the command on all devices containing a specified sub-string in their hostname <ul style="list-style-type: none"> <li>&lt;SUB-STRING&gt; - Specify the sub-string to match. The startup configuration file is erased on all devices whose hostname contains the sub-string specified here.</li> </ul> </li> <li>• exclude-controllers - Optional. Executes the command on all devices excluding controllers. The startup configuration file is erased on all devices except controllers.</li> <li>• exclude-rf-domain-manager - Optional. Executes the command on all devices excluding RF Domain managers. The startup configuration file is erased on all devices except RF Domain managers.</li> <li>• filter &lt;DEVICE-TYPE&gt; - Optional. Executes the command on all devices of a specified type. <ul style="list-style-type: none"> <li>&lt;DEVICE-TYPE&gt; - Specify the device type. The options are: AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533, RFS 4000, NX 5500, NX 7500, NX 95XX, NX 96XX, and VX 9000. The startup configuration file is erased on all devices of the type specified here. For example, if AP7602 is the device-type specified, the startup configuration file on all AP7602, within the RF Domain, is erased.</li> </ul> </li> </ul> </li> </ul> |

## Examples

```
nx9500-6C8809#erase ?
cf: Erase everything in cf:
flash: Erase everything in flash:
nvram: Erase everything in nvram:
startup-config Reset configuration to factory default
usb1: Erase everything in usb1:
usb2: Erase everything in usb2:
nx9500-6C8809#
```

### *exit (privi exec mode)*

Ends the current CLI session and closes the session window

For more information, see [exit](#).

### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6532, AP 6562, AP 7502, AP 7522, AP 7532, AP 7161, AP 81XX, AP 8232
- Wireless Controllers — RFS 4000, RFS 6000
- Service Platforms — NX 7500, NX 9500, NX 9510

### **Syntax**

```
exit
```

### **Parameters**

None

### **Examples**

```
<exsw1>#exit
```

### *ex3500*

Enables EX3500 switch firmware management. Use this command to perform the following operations: boot, copy, delete, and IP-related configurations.

The copy keyword provides multiple copy options. It allows you to upload or download code images or configuration files between the switch's flash memory and an FTP/TFTP server. When you save the system code or configuration settings to a file on an FTP/TFTP server, that file can later be downloaded to the switch to restore system operation. The success of the file transfer depends on the accessibility of the FTP/TFTP server and the quality of the network connection.

### **Supported in the following platforms:**

- Service Platforms — NX 95XX, NX 96XX, VX 9000

## Syntax

```
ex3500 [adoptd|boot|copy|delete|ip]
ex3500 adoptd upgrade <URL> on <EX3500-DEVICE-NAME>
ex3500 boot system <1-1> (config|opcode) <FILE-NAME> on <EX3500-DEVICE-NAME>
ex3500 copy [file|ftp|running-config|startup-config|tftp|unit]
ex3500 copy [file file <SOURCE-FILE-NAME> <DEST-FILE-NAME> on <EX3500-DEVICE-NAME>]
ex3500 copy [ftp|tftp] [add-to-running-config|file|https-certificate|public-key|
running-config|startup-config]
ex3500 copy [ftp|tftp] add-to-running-config <FTP/TFTP-SERVER-IP> <USER-NAME>
<PASSWORD> <SOURCE-FILE-NAME> on <EX3500-DEVICE-NAME>
ex3500 copy [ftp|tftp] file <FTP/TFTP-SERVER-IP> <USER-NAME> <PASSWORD> [1|2]
<SOURCE-FILE-NAME> <DEST-FILE-NAME> on <EX3500-DEVICE-NAME>
ex3500 copy [ftp|tftp] https-certificate <FTP/TFTP-SERVER-IP> <USER-NAME> <PASSWORD>
<SOURCE-CERT-FILE-NAME> <SOURCE-PVT-KEY-FILE-NAME> <PVT-PASS-WORD> on <EX3500-DEVICE-NAME>
ex3500 copy [ftp|tftp] public-key <FTP/TFTP-SERVER-IP> <USER-NAME> <PASSWORD> [1|2]
<SOURCE-PUB-KEY-FILE-NAME> <USER-NAME> on <EX3500-DEVICE-NAME>
ex3500 copy [ftp|tftp] [running-config|startup-config] <FTP/TFTP-SERVER-IP> <USER-NAME>
<PASSWORD>
<SOURCE-CONFIG-FILE-NAME> on <EX3500-DEVICE-NAME>
ex3500 copy running-config [file <DEST-FILE-NAME>|ftp <FTP-SERVER-IP> <USER-NAME>
<PASSWORD>
<DEST-FILE-NAME>|startup-config|tftp <TFTP-SERVER-IP> <DEST-FILE-NAME>] on <EX3500-DEVICE-
NAME>
ex3500 copy startup-config [file <DEST-FILE-NAME>|ftp <FTP-SERVER-IP> <USER-NAME>
<PASSWORD>
<DEST-FILE-NAME>|running-config|tftp <TFTP-SERVER-IP> <DEST-FILE-NAME>] on <EX3500-DEVICE-
NAME>
ex3500 copy unit file <1-1> [1|2] <SOURCE-FILE-NAME> <DEST-FILE-NAME> on <EX3500-DEVICE-
NAME>
ex3500 delete [file|public-key]
ex3500 delete file [name <FILE-NAME>|unit <1-1> name <FILE-NAME>] on <EX3500-DEVICE-NAME>
ex3500 delete public-key <USER-NAME> [dsa|rsa] on <EX3500-DEVICE-NAME>
ex3500 ip ssh [crypto|save]
ex3500 ip ssh crypto host-key generates [dsa|rsa] on <EX3500-DEVICE-NAME>
ex3500 ip ssh crypto zeroize [dsa|rsa] on <EX3500-DEVICE-NAME>
ex3500 ip ssh save host-key on <EX3500-DEVICE-NAME>
```

## Parameters

```
ex3500 adoptd upgrade <URL> on <EX3500-DEVICE-NAME>
```

|                         |                                                                                                                                                                                                                                                     |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ex3500 adoptd upgrade   | Upgrades an adopted EX3500 switch After an upgrade, reboot the EX3500 switch to initiate the new image.<br><br><b>Note:</b> To view an EX3500's current image version, use the <b>show &gt; version &gt; on &lt;EX3500-DEVICE-NAME&gt;</b> command. |
| <URL>                   | Specifies the location and image file name in the following format: tftp://<IP>[/path]/file                                                                                                                                                         |
| on <EX3500-DEVICE-NAME> | Executes the command on a specified EX3500 switch <ul style="list-style-type: none"><li>&lt;EX3500-DEVICE-NAME&gt; - Specify the EX3500 switch's hostname.</li></ul>                                                                                |

```
ex3500 boot system <1-1> (config|opcode) <FILE-NAME> on <EX3500-DEVICE-NAME>
```

|                    |                                                                                                                                                                                |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ex3500 boot system | Boots a EX3500 switch using a specified configuration file                                                                                                                     |
| <1-1>              | Identifies the EX3500 unit by its ID number. Specify the EX3500 ID from 1 - 1.<br><br><b>Note:</b> As of now only one (1) EX3500 unit can be managed through a NOC controller. |

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| (config opcode) <FILE-NAME> | <p>The following keywords are recursive: Specifies the image file to use for booting. The options are:</p> <ul style="list-style-type: none"> <li>• config - Uses the configuration file to boot the switch</li> <li>• opcode - Uses the <i>Operation Code</i> (opcode), which is the runtime code, to boot the switch. The opcode is like an operating system that enables the WiNG software to communicate with the EX3500 device.</li> </ul> <p>The following parameter is common to the 'config' and opcode' keywords:</p> <ul style="list-style-type: none"> <li>• &lt;FILE-NAME&gt; - Specify the configuration/runtime-code file name.</li> </ul> |
| on <EX3500-DEVICE-NAME>     | <p>Reloads a specified EX3500 switch</p> <ul style="list-style-type: none"> <li>• &lt;EX3500-DEVICE-NAME&gt; - Specify the EX3500 switch's hostname. You can also specify its MAC address.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

ex3500 copy file file <SOURCE-FILE-NAME> <DEST-FILE-NAME> on <EX3500-DEVICE-NAME>

|                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ex3500 copy                                   | Copies a configuration file to another file                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| file file <SOURCE-FILE-NAME> <DEST-FILE-NAME> | <p>Copies a specified file (this is the source configuration file)</p> <ul style="list-style-type: none"> <li>• file - Copies the specified source file to a specified file (this is the destination configuration file)</li> <li>• &lt;SOURCE-FILE-NAME&gt; - Specify the source configuration file's name</li> <li>• &lt;DEST-FILE-NAME&gt; - Specify the destination configuration file's name.</li> </ul> <p>When specifying the destination file name, keep in mind the following points:</p> <ul style="list-style-type: none"> <li>- It should not contain slashes (\ or /),</li> <li>- It should not exceed 32 characters for files on the switch, or 127 characters for files on the server.</li> </ul> |
| on <EX3500-DEVICE-NAME>                       | <p>Copies the file to a specified EX3500 switch</p> <ul style="list-style-type: none"> <li>• &lt;EX3500-DEVICE-NAME&gt; - Specify the EX3500 switch's hostname. The specified source file is copied to specified destination file on the EX3500 identified here.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                      |

ex3500 copy [ftp|tftp] add-to-running-config <FTP/TFTP-SERVER-IP> <USER-NAME> <PASSWORD> <SOURCE-FILE-NAME> on <EX3500-DEVICE-NAME>

|                        |                                                                                                                                                                                                                                                                                                                        |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ex3500 copy [ftp tftp] | <p>Copies files from a FTP or TFTP server. This command allows you to copy the following types of files: HTTPS certificate, running configuration, startup configuration, public key, etc.</p> <p>This command also allows you to add a remote system's running configuration to the current system configuration.</p> |
| add-to-running-config  | Adds a remote system's running configuration to the current system                                                                                                                                                                                                                                                     |

|                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <FTP/TFTP-SERVER-IP><br><USER-NAME><br><PASSWORD> | Configures the FTP or TFTP server details (depending on the option selected in the previous step), such as IP address and user credentials. This is the device running the FTP/TFTP server. <ul style="list-style-type: none"> <li>• &lt;FTP/TFTP-SERVER-IP&gt; - Specify the FTP or TFTP server's IP address in the A.B.C.D format.</li> <li>• &lt;USER-NAME&gt; - If using a FTP server, specify the FTP server's user name (should be an authorized user)</li> <li>• &lt;PASSWORD&gt; - Specify the password applicable for the above specified FTP server user name.</li> </ul> |
| <SOURCE-FILE-NAME>                                | After specifying the server details, specify the name of the running configuration file. <ul style="list-style-type: none"> <li>• &lt;SOURCE-FILE-NAME&gt; - Specify the source file's name.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                             |
| on <EX3500-DEVICE-NAME>                           | Copies the file to a specified EX3500 switch <ul style="list-style-type: none"> <li>• &lt;EX3500-DEVICE-NAME&gt; - Specify the EX3500 switch's hostname. The specified source file is copied to specified destination file on the EX3500 identified here.</li> </ul>                                                                                                                                                                                                                                                                                                                |

```
ex3500 copy [ftp|tftp] file <FTP/TFTP-SERVER-IP> <USER-NAME> <PASSWORD> [1|2] <SOURCE-FILE-NAME> <DEST-FILE-NAME> on <EX3500-DEVICE-NAME>
```

|                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ex3500 copy [ftp tftp]                         | Copies files from a FTP or TFTP server. This command allows you to copy the following types of files: HTTPS certificate, running configuration, startup configuration, public key, etc.                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| file                                           | Copies to a specified file system                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <FTP/TFTP-SERVER-IP><br><USER-NAME> <PASSWORD> | Configures the FTP or TFTP server details (depending on the option selected in the previous step), such as IP address and user credentials. This is the device running the FTP/TFTP server. <ul style="list-style-type: none"> <li>• &lt;FTP/TFTP-SERVER-IP&gt; - Specify the FTP or TFTP server's IP address in the A.B.C.D format.</li> <li>• &lt;USER-NAME&gt; - If using a FTP server, specify the FTP server's user name (should be an authorized user)</li> <li>• &lt;PASSWORD&gt; - Specify the password applicable for the above specified FTP server user name.</li> </ul>                                                           |
| [1 2] <SOURCE-FILE-NAME> <DEST-FILE-NAME>      | After specifying the server details, select the file type and specify the name of the source and destination file names. <ul style="list-style-type: none"> <li>• [1 2] - Select the file type from 1 - 2. <ul style="list-style-type: none"> <li>• 1 - Copies the EX3500 configuration file.</li> <li>• 2 - Copies the opcode, which is the runtime code. The opcode is like an operating system that enables the WiNG software to communicate with the EX3500 device.</li> </ul> </li> <li>• &lt;SOURCE-FILE-NAME&gt; - Specify the source file's name.</li> <li>• &lt;DEST-FILE-NAME&gt; - Specify the destination file's name.</li> </ul> |
| on <EX3500-DEVICE-NAME>                        | Copies the file to a specified EX3500 device <ul style="list-style-type: none"> <li>• &lt;EX3500-DEVICE-NAME&gt; - Specify the EX3500 device's hostname. The specified source file is copied to specified destination file on the EX3500 identified here.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                          |

```
ex3500 copy [ftp|tftp] https-certificate <FTP/TFTP-SERVER-IP> <USER-NAME> <PASSWORD> <SOURCE-CERT-FILE-NAME> <SOURCE-PVT-KEY-FILE-NAME> <PVT-PASS-WORD> on <EX3500-DEVICE-NAME>
```

|                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ex3500 copy [ftp tftp]                                             | Copies files from a FTP or TFTP server. This command allows you to copy the following types of files: HTTPS certificate, running configuration, startup configuration, public key, etc.                                                                                                                                                                                                                                                                                                                                                                                             |
| https-certificate                                                  | Copies HTTPS secure site certificate from the FTP or TFTP server to the switch                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <FTP/TFTP-SERVER-IP><br><USER-NAME><br><PASSWORD>                  | Configures the FTP or TFTP server details (depending on the option selected in the previous step), such as IP address and user credentials. This is the device running the FTP/TFTP server. <ul style="list-style-type: none"> <li>• &lt;FTP/TFTP-SERVER-IP&gt; - Specify the FTP or TFTP server's IP address in the A.B.C.D format.</li> <li>• &lt;USER-NAME&gt; - If using a FTP server, specify the FTP server's user name (should be an authorized user)</li> <li>• &lt;PASSWORD&gt; - Specify the password applicable for the above specified FTP server user name.</li> </ul> |
| <SOURCE-CERT-FILE-NAME> <SOURCE-PVT-KEY-FILE-NAME> <PVT-PASS-WORD> | After identifying the FTP or TFTP server, specify the following: <ul style="list-style-type: none"> <li>• &lt;SOURCE-CERT-FILE-NAME&gt; - Specify the source HTTPS secure site certificate file name.</li> <li>• &lt;SOURCE-PVT-KEY-FILE-NAME&gt; - Specify the source private-key file name.</li> <li>• &lt;PVT-PASS-WORD&gt; - Specify the private password.</li> </ul>                                                                                                                                                                                                           |
| on <EX3500-DEVICE-NAME>                                            | Copies the file to a specified EX3500 device <ul style="list-style-type: none"> <li>• &lt;EX3500-DEVICE-NAME&gt; - Specify the EX3500 device's hostname.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                 |

```
ex3500 copy [ftp|tftp] public-key <FTP/TFTP-SERVER-IP> <USER-NAME> <PASSWORD> [1|2]
<SOURCE-PUB-KEY-FILE-NAME> <USER-NAME> on <EX3500-DEVICE-NAME>
```

|                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ex3500 copy [ftp tftp]                         | Copies files from a FTP or TFTP server. This command allows you to copy the following types of files: HTTPS certificate, running configuration, startup configuration, public key, etc.                                                                                                                                                                                                                                                                                                                                                                                             |
| public-key                                     | Copies the SSH public key from the FTP or TFTP server to the switch                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <FTP/TFTP-SERVER-IP><br><USER-NAME> <PASSWORD> | Configures the FTP or TFTP server details (depending on the option selected in the previous step), such as IP address and user credentials. This is the device running the FTP/TFTP server. <ul style="list-style-type: none"> <li>• &lt;FTP/TFTP-SERVER-IP&gt; - Specify the FTP or TFTP server's IP address in the A.B.C.D format.</li> <li>• &lt;USER-NAME&gt; - If using a FTP server, specify the FTP server's user name (should be an authorized user)</li> <li>• &lt;PASSWORD&gt; - Specify the password applicable for the above specified FTP server user name.</li> </ul> |

|                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [1 2] <SOURCE-PUB-KEY-FILE-NAME> <USER-NAME> | <p>After identifying the FTP or TFTP server, specify the following:</p> <ul style="list-style-type: none"> <li>[1 2] – Configures the SSH public key type as RS or DSA <ul style="list-style-type: none"> <li>1 – Configures the public key type as RSA</li> <li>2 – Configures the public key type as DSA</li> </ul> </li> <li>&lt;SOURCE-PUB-KEY-FILE-NAME&gt; – Specifies the source public key file name</li> <li>&lt;USER-NAME&gt; – Specifies the public key's user name</li> </ul> |
| on <EX3500-DEVICE-NAME>                      | <p>Copies the public key to a specified EX3500 device</p> <ul style="list-style-type: none"> <li>&lt;EX3500-DEVICE-NAME&gt; – Specify the EX3500 device's hostname.</li> </ul>                                                                                                                                                                                                                                                                                                            |

```
ex3500 copy [ftp|tftp] [running-config|startup-config] <FTP/TFTP-SERVER-IP> <USER-NAME>
<PASSWORD> <DEST-FILE-NAME> on <EX3500-DEVICE-NAME>
```

|                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ex3500 copy [ftp tftp]                            | Copies files from a FTP or TFTP server. This command allows you to copy the following types of files: HTTPS certificate, running configuration, startup configuration, public key, etc.                                                                                                                                                                                                                                                                       |
| [running-config] startup-config]                  | Copies the running or startup configuration file to one of the following destinations: file system, FTP server, or TFTP server<br>The running configuration file can be copied to the startup configuration file and vice versa.                                                                                                                                                                                                                              |
| <FTP/TFTP-SERVER-IP><br><USER-NAME><br><PASSWORD> | <p>If copying to a FTP/TFTP server, configure the following parameters:</p> <ul style="list-style-type: none"> <li>&lt;FTP/TFTP-SERVER-IP&gt; – Specify the FTP or TFTP server's IP address in the A.B.C.D format.</li> <li>&lt;USER-NAME&gt; – If using a FTP server, specify the FTP server's user name (should be an authorized user)</li> <li>&lt;PASSWORD&gt; – Specify the password applicable for the above specified FTP server user name.</li> </ul> |
| <DEST-FILE-NAME>                                  | <p>Configures the destination file name. The running or startup configuration file is copied to the specified destination file.</p> <ul style="list-style-type: none"> <li>&lt;DEST-FILE-NAME&gt; – Specify the destination file name. You can also copy the running configuration file to the startup configuration file and vice versa.</li> </ul>                                                                                                          |
| on <EX3500-DEVICE-NAME>                           | <p>Copies the running or startup configuration file on to a specified EX3500 device</p> <ul style="list-style-type: none"> <li>&lt;EX3500-DEVICE-NAME&gt; – Specify the EX3500 device's hostname.</li> </ul>                                                                                                                                                                                                                                                  |

```
ex3500 copy unit file <1-1> [1|2] <SOURCE-FILE-NAME> <DEST-FILE-NAME> on <EX3500-DEVICE-NAME>
```

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ex3500 copy unit   | Copies from a EX3500 switch                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| file <1-1> [1 2]   | <p>Copies the file system from the EX3500 switch identified by the unit number</p> <ul style="list-style-type: none"> <li>&lt;1-1&gt; – Specify the unit number from 1 - 1. <ul style="list-style-type: none"> <li>[1 2] – Select the file type from 1 - 2. 1 - Copies the selected unit's configuration file.</li> <li>2 – Copies the selected unit's opcode, which is the runtime code. The opcode is like an operating system that enables the WING software to communicate with the EX3500 device.</li> </ul> </li> </ul> |
| <SOURCE-FILE-NAME> | <p>Configures the source file name</p> <ul style="list-style-type: none"> <li>&lt;SOURCE-FILE-NAME&gt; – Specify the source file name. You can copy the running configuration file to the startup configuration file and vice versa.</li> </ul>                                                                                                                                                                                                                                                                               |



|                         |                                                                                                                                                                                                                                                                                                                                |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <DEST-FILE-NAME>        | Configures the destination file name. The running or startup configuration file is copied to the specified file. <ul style="list-style-type: none"> <li>• &lt;DEST-FILE-NAME&gt; - Specify the destination file name. You can copy the running configuration file to the startup configuration file and vice versa.</li> </ul> |
| on <EX3500-DEVICE-NAME> | Copies the running or startup configuration file on to a specified EX3500 device <ul style="list-style-type: none"> <li>• &lt;EX3500-DEVICE-NAME&gt; - Specify the EX3500 device's hostname.</li> </ul>                                                                                                                        |

```
ex3500 delete file [name <FILE-NAME>|unit <1-1> name <FILE-NAME>] on <EX3500-DEVICE-NAME>
```

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ex3500 delete file          | Deletes a file or image on a specified EX3500 device                                                                                                                                                                                                                                                                                                                                                                      |
| name <FILE-NAME>            | Specifies the file to delete. The specified file is deleted. <ul style="list-style-type: none"> <li>• &lt;FILE-NAME&gt; - Specify the file name.</li> </ul>                                                                                                                                                                                                                                                               |
| unit <1-1> name <FILE-NAME> | Identifies the unit in the stackable system on which the file is located <ul style="list-style-type: none"> <li>• &lt;1-1&gt; - Select the unit from 1 - 1. <ul style="list-style-type: none"> <li>• name - After identifying the unit, specify the file to delete. The specified file is deleted. <ul style="list-style-type: none"> <li>• &lt;FILE-NAME&gt; - Specify the file name.</li> </ul> </li> </ul> </li> </ul> |
| on <EX3500-DEVICE-NAME>     | Executes the command on a specified EX3500 device <ul style="list-style-type: none"> <li>• &lt;EX3500-DEVICE-NAME&gt; - Specify the EX3500 device's hostname.</li> </ul>                                                                                                                                                                                                                                                  |

```
ex3500 delete public-key <USER-NAME> [dsa|rsa] on <EX3500-DEVICE-NAME>
```

|                                                   |                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ex3500 delete public-key<br><USER-NAME> [dsa rsa] | Deletes a specified user's public key <ul style="list-style-type: none"> <li>• &lt;USER-NAME&gt; - Specify the SSH user's name. <ul style="list-style-type: none"> <li>• dsa - Deletes the specified user's DSA (version 2) key</li> <li>• rsa - Deletes the specified user's RSA (version 1) key</li> </ul> </li> </ul> |
| on <EX3500-DEVICE-NAME>                           | Executes the command on a specified EX3500 device <ul style="list-style-type: none"> <li>• &lt;EX3500-DEVICE-NAME&gt; - Specify the EX3500 device's hostname.</li> </ul>                                                                                                                                                 |

```
ex3500 ip ssh crypto host-key generates [dsa|rsa] on <EX3500-DEVICE-NAME>
```

|                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ex3500 ip ssh crypto host-key generates [dsa rsa] | <p>Generates the host-key pair (public and private). This host key is used by the SSH server to negotiate a session key and encryption method with the client trying to connect to it.</p> <ul style="list-style-type: none"> <li>• dsa – Generates DSA (version 2) key type</li> <li>• rsa – Generates RSA (version 1) key type</li> </ul> <p><b>Note:</b> The RSA Version 1 is used only for SSHv1.5 clients, whereas DSA Version 2 is used only for SSHv2 clients.</p> <p><b>Note:</b> This generated host-key pair is stored in the volatile memory (i.e RAM). To save the host-key pair in the flash memory, use the <b>ex3500 &gt; ip &gt; ssh &gt; save &gt; host-key</b> command.</p> |
| on <EX3500-DEVICE-NAME>                           | <p>Executes the command on a specified EX3500 device</p> <ul style="list-style-type: none"> <li>• &lt;EX3500-DEVICE-NAME&gt; – Specify the EX3500 device's hostname.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

```
ex3500 ip ssh zeroize [dsa|rsa] <EX3500-DEVICE-NAME>
```

|                                 |                                                                                                                                                                                 |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ex3500 ip ssh zeroize [dsa rsa] | Removes the host-key (DSA and RSA) from the volatile memory (i.e. RAM)                                                                                                          |
| on <EX3500-DEVICE-NAME>         | <p>Executes the command on a specified EX3500 device</p> <ul style="list-style-type: none"> <li>• &lt;EX3500-DEVICE-NAME&gt; – Specify the EX3500 device's hostname.</li> </ul> |

```
ex3500 ip ssh save host-key on <EX3500-DEVICE-NAME>
```

|                             |                                                                                                                                                                                 |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ex3500 ip ssh save host-key | Saves the host-key (DSA and RSA) to the flash memory                                                                                                                            |
| on <EX3500-DEVICE-NAME>     | <p>Executes the command on a specified EX3500 device</p> <ul style="list-style-type: none"> <li>• &lt;EX3500-DEVICE-NAME&gt; – Specify the EX3500 device's hostname.</li> </ul> |

### Usage Guidelines

When using the ex3500 command and its parameters, keep in mind the following:

- Destination file names should not:
  - Contain slashes (\ or /),
  - Exceed 32 characters for files on the switch, or 127 characters for files on the server.
- The FTP server's default user name is set as "anonymous".
- The Boot ROM and Loader cannot be uploaded or downloaded from the FTP/TFTP server. Follow instructions provided in the release notes for new firmware, or contact your distributor for help.
- The "Factory\_Default\_Configure" can be used as the source to copy from, but cannot be used as the destination.
- Although the switch supports only two operation code files, the maximum number of user-defined configuration files supported is 16.

### Example

```

nx9500-6C8809#ex3500 adopted upgrade tftp://192.168.0.99/ex3500-adopted-5.8.5.0.img on
ex3524-ED5EAC
Flash programming started
Flash programming completed
Successful
nx9500-6C8809#
nx9500-6C8809#ex3500 copy tftp file 10.2.0.100 1 m360.bix m360.bix on ex3524-ED5EAC
\Write to FLASH Programming.
```

```

-Write to FLASH finish.
Success.
nx9500-6C8809#
nx9500-6C8809#ex3500 copy tftp startup-config 10.2.0.99 startup.01 startup on ex3524-ED5EAC
TFTP server ip address: 10.1.0.99
Flash programming started.
Flash programming completed.
Success.
nx9500-6C8809#

```

## factory-reset

Erases startup configuration on a specified device or all devices within a specified RF Domain

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```

factory-reset [<HOSTNAME/MAC>|config-all|config-device-only|on <RF-DOMAIN-NAME>]
factory-reset <HOSTNAME/MAC> {<HOSTNAME/MAC>}
factory-reset on <RF-DOMAIN-NAME> {containing <SUB-STRING>/exclude-controllers/
exclude-rf-domain-manager/filter <DEVICE-TYPE>}
factory-reset [config-all|config-device-only] [<HOSTNAME/MAC> {<HOSTNAME/MAC>}|on <RF-
DOMAIN-NAME>
{containing <SUB-STRING>/exclude-controllers/exclude-rf-domain-manager/filter <DEVICE-
TYPE>}]

```

### Parameters

```
factory-reset <HOSTNAME/MAC> {<HOSTNAME/MAC>}
```

|                                    |                                                                                                                                                                                                                                                |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| factory-reset                      | Erases startup configuration and reloads device(s) based on the parameters passed<br>For more information on the actions performed by this command, see <a href="#">Actions performed by the factory-reset command</a> .                       |
| <HOSTNAME/MAC><br>{<HOSTNAME/MAC>} | Erases startup configuration and reloads the device identified by the <HOSTNAME/MAC> keyword <ul style="list-style-type: none"> <li>• &lt;HOSTNAME/MAC&gt; - Optional. You can optionally specify multiple space-separated devices.</li> </ul> |

```
factory-reset on <RF-DOMAIN-NAME> {containing <SUB-STRING>/exclude-controllers/
exclude-rf-domain-manager/filter <DEVICE-TYPE>}
```

|                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>factory-reset</p> <p>on &lt;RF-DOMAIN-NAME&gt;<br/>{containing &lt;SUB-STRING&gt; <br/>exclude-controllers <br/>exclude-rf-domain-<br/>manager  filter &lt;DEVICE-<br/>TYPE&gt;}]</p> | <p>Erases startup configuration and reloads device(s) based on the parameters passed<br/>For more information on the actions performed by this command, see <a href="#">Actions performed by the factory-reset command</a>.</p> <p>Erases startup configuration and reloads all devices or specified device(s) within a specified RF Domain identified by the &lt;RF-DOMAIN-NAME&gt; keyword</p> <ul style="list-style-type: none"> <li>• &lt;RF-DOMAIN-NAME&gt; – Specify the RF Domain name. After specifying the RF Domain, optionally use the filters provided to identify specific device(s) within the RF Domain. If none of the filters are used, the command is executed on all devices within the RF Domain. These filters are: <ul style="list-style-type: none"> <li>• containing &lt;SUB-STRING&gt; – Optional. Executes the command on all devices containing a specified sub-string in their hostname<br/>    &lt;SUB-STRING&gt; – Specify the sub-string to match.</li> <li>• exclude-controllers – Optional. Executes the command on all devices excluding controllers. Since only a NOC controller is capable of adopting other controllers, use this option when executing the command on a NOC controller.</li> <li>• exclude-rf-domain-manager – Optional. Executes the command on all devices excluding RF Domain managers. Use this option when executing the command on the NOC, site controller, or RF Domain manager.</li> <li>• filter &lt;DEVICE-TYPE&gt; – Optional. Executes the command on all devices of a specified type<br/>    &lt;DEVICE-TYPE&gt; – Specify the device type. The options are:AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533, RFS 4000, NX 5500, NX 75XX, NX 95XX, NX 96XX, and VX 9000. The startup configuration is erased on all devices of the type specified here. For example, if AP 7602 is the device-type specified, the command is executed on all AP 7602s within the specified RF Domain.</li> </ul> </li> </ul> |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
factory-reset [config-all|config-device-only] [<HOSTNAME/MAC> {<HOSTNAME/MAC>}]on <RF-DOMAIN-NAME>
{containing <SUB-STRING>|exclude-controllers|exclude-rf-domain-manager|filter <DEVICE-TYPE>}]
```

|                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>factory-reset</p> <p>[config-all  config-device-<br/>only]</p> | <p>Erases startup configuration and reloads device(s) based on the parameters passed<br/>For more information on the actions performed by this command, see <a href="#">Actions performed by the factory-reset command</a>.</p> <p>Erases startup configuration and reloads only controller-adopted devices or the controller as well as its adopted devices</p> <ul style="list-style-type: none"> <li>• config-all – Erases startup configuration on the controller and all devices adopted by it</li> <li>• config-device-only – Erases startup configuration only on the devices adopted by the controller</li> </ul> |
|-------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>&lt;HOSTNAME/MAC&gt;<br/>{&lt;HOSTNAME/MAC&gt;}</p>                                                                                       | <p>This parameter is common to the 'config-all' and 'config-device-only' keywords:</p> <ul style="list-style-type: none"> <li>• &lt;HOSTNAME/MAC&gt; - Erases startup configuration and reloads the device identified by the &lt;HOSTNAME/MAC&gt; keyword. Specify the device's hostname or MAC address.</li> <li>• &lt;HOSTNAME/MAC&gt; - Optional. You can optionally specify multiple space-separated devices.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <p>on &lt;RF-DOMAIN-NAME&gt;<br/>{containing &lt;SUB-STRING&gt; exclude-controllers exclude-rf-domain-manager filter &lt;DEVICE-TYPE&gt;</p> | <p>The following parameters are common to the 'config-all' and 'config-device-only' keywords:</p> <ul style="list-style-type: none"> <li>• on &lt;RF-DOMAIN-NAME&gt; - Erases startup configuration and reloads all devices or specified device(s) within a specified RF Domain</li> <li>• &lt;RF-DOMAIN-NAME&gt; - Specify the RF Domain name.</li> </ul> <p>After specifying the RF Domain, optionally use the filters provided to identify specific device(s) within the RF Domain. If none of the filters are used, the command is executed on all devices within the RF Domain. These filters are:</p> <ul style="list-style-type: none"> <li>containing &lt;SUB-STRING&gt; - Optional. Executes the command on all devices containing a specified sub-string in their hostname <ul style="list-style-type: none"> <li>&lt;SUB-STRING&gt; - Specify the sub-string to match.</li> </ul> </li> <li>exclude-controllers - Optional. Executes the command on all devices excluding controllers. Since only a NOC controller is capable of adopting other controllers, use this option when executing the command on a NOC controller.</li> <li>exclude-rf-domain-manager - Optional. Executes the command on all devices excluding RF Domain managers. Use this option when executing the command on the NOC, Site controller, or RF Domain manager.</li> <li>filter &lt;DEVICE-TYPE&gt; - Optional. Executes the command on all devices of a specified type <ul style="list-style-type: none"> <li>&lt;DEVICE-TYPE&gt; - Specify the device type. The options are: AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533, RFS 4000, NX 5500, NX 75XX, NX 95XX, NX 96XX, and VX 9000.</li> </ul> </li> </ul> |

### Usage Guidelines (Actions performed by the factory-reset command)

The action taken by this command depends on the parameters passed.

- For the **factory-reset** [**<DEVICE-NAME>** | **on <RF-DOMAIN-NAME>**] options, the command:
  - Erases startup configuration on the target device (or) all devices in the target RF Domain.
  - Erases the device configuration entries from the controller's configuration for the target device (or) for all the devices in the target RF Domain.
  - Reloads the target device (or) all devices in the target RF Domain.
- For the **factory-reset config-all** [**<DEVICE-NAME>** | **on <RF-DOMAIN-NAME>**] options, the command:
  - Erases startup configuration on the target device (or) all devices in the target RF Domain.
  - Erases the device configuration entries from the controller's configuration for the target device (or) for all the devices in the target RF Domain.
- For the **factory-reset config-device-only** [**<DEVICE-NAME>** | **on <RF-DOMAIN-NAME>**] options, the command:
  - Erases startup configuration on the target device (or) all devices in the target RF Domain.

## Example

```
nx7500-7F3609#factory-reset config-all ap6522-5A873C
In progress
Erased startup-config - success 1 fail 0
Successful device deletion - total 1
nx7500-7F3609#
rfs4000-6DB5D4# factory-reset B4-C7-99-5A-87-3C
In progress
Erased startup-config and initiated reload - success 1 fail 0
Successful device deletion - total 1
rfs4000-6DB5D4#
```

### *file-sync (user and privi exec modes)*

Syncs trustpoint and/or EAP-TLS X.509 (PKCS#12) certificate between the staging-controller and adopted access points.

When enabling file syncing, consider the following points:

- The X.509 certificate needs synchronization only if the access point is configured to use EAP-TLS authentication.
- Execute the command on the controller adopting the access points.
- Ensure that the X.509 certificate file is installed on the controller.

Syncing of trustpoint/wireless-bridge certificate can be automated. To automate file syncing, in the controller's device/profile configuration mode, execute the following command: **file-sync [auto|count <1-20>]**. For more information, see [file-sync](#) on page 999.



### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
file-sync [cancel|load-file|trustpoint|wireless-bridge]
file-sync cancel [trustpoint|wireless-bridge]
file-sync cancel [trustpoint|wireless-bridge] [<DEVICE-NAME>|all|rf-domain [<DOMAIN-NAME>|all]]
file-sync load-file [trustpoint|wireless-bridge]
file-sync load-file [trustpoint <TRUSTPOINT-NAME>|wireless-bridge] <URL>
file-sync [trustpoint <TRUSTPOINT-NAME>|wireless-bridge] [<DEVICE-NAME>|all|rf-domain [<DOMAIN-NAME>|all]] {from-controller} {reset-radio/upload-time <TIME>}
```

### Parameters

```
file-sync cancel [trustpoint|wireless-bridge] [<DEVICE-NAME>|all|rf-domain [<DOMAIN-NAME>|all]]
```

```
file-sync cancel [trustpoint|
wireless-bridge] [<DEVICE-
NAME>|all|rf-domain
[<DOMAIN-NAME>|all]]
```

Cancels scheduled file synchronization

- trustpoint – Cancels scheduled trustpoint synchronization on a specified AP, all APs, or APs within a specified RF Domain
- wireless-bridge – Cancels scheduled wireless-bridge certificate synchronization on a specified AP, all APs, or APs within a specified RF Domain
  - <DEVICE-NAME> – Cancels scheduled trustpoint/certificate synchronization on a specified AP. Specify the AP's hostname or MAC address.
  - all – Cancels scheduled trustpoint/certificate synchronization on all APs
  - rf-domain [<DOMAIN-NAME>|all] – Cancels scheduled trustpoint/certificate synchronization on all APs in a specified RF Domain or in all RF Domains
    - <DOMAIN-NAME> – Cancels scheduled trustpoint/certificate synchronization on all APs within a specified RF Domain. Specify the RF Domain's name.
    - all – Cancels scheduled trustpoint/certificate synchronization on all RF Domains

```
file-sync load-file [trustpoint|wireless-bridge] <URL>
```

```
file-sync load-file [trustpoint|
wireless-bridge] <URL>
```

Loads the following files on to the staging controller:

- trustpoint – Loads the trustpoint, including CA certificate, server certificate and private key
- wireless-bridge – Loads the wireless-bridge certificate to the staging controller. Use this command to load the certificate to the controller before scheduling or initiating a certificate synchronization.
- <URL> – Provide the trustpoint/certificate location using one of the following formats:

```
tftp://<hostname|IP>[:port]/path/file
```

```
ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file
```

```
sftp://<user>:<passwd>@<hostname|IP>[:port]/path/file
```

```
http://<hostname|IP>[:port]/path/file
```

**Note:** Both IPv4 and IPv6 address types are supported.

```
cf:/path/file
```

```
usb<n>:/path/file
```

```
file-sync [trustpoint <TRUSTPOINT-NAME>|wireless-bridge] [<DEVICE-NAME>|
all|rf-domain [<DOMAIN-NAME>|all]] {from-controller} {reset-radio|upload-time <TIME>}
```

|                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>file-sync trustpoint &lt;TRUSTPOINT-NAME&gt; [&lt;DEVICE-NAME&gt;] all rf- domain [&lt;DOMAIN-NAME&gt;  all] from-controller]</pre> | <p>Configures file-syncing parameters</p> <ul style="list-style-type: none"> <li>trustpoint &lt;TRUSTPOINT-NAME&gt; - Syncs a specified trustpoint between controller and its adopted APs <ul style="list-style-type: none"> <li>&lt;TRUSTPOINT-NAME&gt; - Specify the trustpoint name.</li> </ul> </li> <li>wireless-bridge - Syncs wireless-bridge certificate between controller and its adopted APs</li> </ul> <p>After specifying the file that is to be synced, configure following file-sync parameters:</p> <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; - Syncs trustpoint/certificate with a specified AP. Specify the AP's hostname or MAC address.</li> <li>all - Syncs trustpoint/certificate with all APs</li> <li>rf-domain [&lt;DOMAIN-NAME&gt; all] from-controller - Syncs trustpoint/certificate with all APs in a specified RF Domain or in all RF Domains <ul style="list-style-type: none"> <li>&lt;DOMAIN-NAME&gt; - Select to sync with APs within a specified RF Domain. Specify the RF Domain's name.</li> <li>all - Select to sync with APs across all RF Domains</li> </ul> </li> </ul> <p>from-controller - Optional. Loads certificate to the APs from the adopting controller and not the RF Domain manager</p> <p>After specifying the access points, specify the following options:<br/><b>reset-radio</b> and <b>upload-time</b>.</p> |
| <pre>reset-radio</pre>                                                                                                                   | <p>This keyword is recursive and applicable to all of the above parameters. Optional. Resets the radio after file synchronization. Reset the radio in case the certificate is renewed along with no changes made to the 'bridge EAP username' and 'bridge EAP password'.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <pre>upload-time &lt;TIME&gt;</pre>                                                                                                      | <p>This keyword is recursive and applicable to all of the above parameters.</p> <ul style="list-style-type: none"> <li>upload-time - Optional. Schedules certificate upload at a specified time <ul style="list-style-type: none"> <li>&lt;TIME&gt; - Specify the time in the MM/DD/YYYY-HH:MM or HH:MM format. If no time is configured, the process is initiated as soon as the command is executed.</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

### Example (User Exec Mode)

```
NOC-NX9500>file-sync wireless-bridge ap7161-11E6C4 upload-time 06/01/2018-12:30
```

| CONTROLLER        | STATUS  | MESSAGE                |
|-------------------|---------|------------------------|
| B4-C7-99-6C-88-09 | Success | Queued 1 APs to upload |

```
NOC-NX9500>
```

The following command uploads certificate to all access points:

```
NOC-NX9500>file-sync wireless-bridge all upload-time 06/01/2018-23:42
```

### Example (Privi Exec Mode)

```
rfs4000-6DB5D4#file-sync wireless-bridge ap7161-11E6C4 upload-time 06/01/2018-12:30
```

| CONTROLLER        | STATUS  | MESSAGE                |
|-------------------|---------|------------------------|
| B4-C7-99-6D-B5-D4 | Success | Queued 1 APs to upload |

```
rfs4000-6DB5D4#
```



The following command uploads certificate to all access points:

```
rfs4000-6DB5D4#file-sync wireless-bridge all upload-time 06/01/2018-23:42
```

## halt

Stops (halts) a device (Access Point, wireless controller, or service platform). Once halted, the system must be restarted manually.

This command stops the device immediately. No indications or notifications are provided while the device shuts down.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
halt force {on <DEVICE-NAME>}
```

### Parameters

```
halt force {on <DEVICE-NAME>}
```

|                                                                                                                                                                                                                                                                               |                                                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| halt                                                                                                                                                                                                                                                                          | Halts a device                                                                                                                               |
| force                                                                                                                                                                                                                                                                         | Optional. Forces a device to halt ignoring in-progress operations, such as firmware upgrades, downloads, unsaved configuration changes, etc. |
| The following keywords are recursive and applicable to the 'force' parameter:                                                                                                                                                                                                 |                                                                                                                                              |
| <ul style="list-style-type: none"><li>• on &lt;DEVICE-NAME&gt; - Optional. Specifies the name of the device to be halted<ul style="list-style-type: none"><li>• &lt;DEVICE-NAME&gt; - Enter the name of the AP, wireless controller, or service platform.</li></ul></li></ul> |                                                                                                                                              |
| <b>Note:</b> If the device name is not specified, the logged device is halted.                                                                                                                                                                                                |                                                                                                                                              |

### Example

```
nx9500-6C8809#halt on rfs4000-229D58
nx9500-6C8809#
```

## join-cluster (user and privi exec modes)

Adds a device (access point, wireless controller, or service platform), as a member, to an existing cluster of devices. Assign a static IP address to the device before adding to a cluster. Note, a cluster can be only formed of devices of the same model type.



### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
join-cluster <IP> user <USERNAME> password <WORD> {level|mode}
join-cluster <IP> user <USERNAME> password <WORD> {level [1|2]|mode [active|standby]}
```

## Parameters

```
join-cluster <IP> user <USERNAME> password <WORD> {level [1|2]|mode [active|standby]}
```

|                       |                                                                                                                                                                                                      |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| join-cluster          | Adds a access point wireless controller, or service platform to an existing cluster                                                                                                                  |
| <IP>                  | Specify the cluster member's IP address.                                                                                                                                                             |
| user <USERNAME>       | Specify a user account with super user privileges on the new cluster member                                                                                                                          |
| password <WORD>       | Specify password for the account specified in the user parameter                                                                                                                                     |
| level [1 2]           | Optional. Configures the routing level <ul style="list-style-type: none"><li>• 1 – Configures level 1 routing</li><li>• 2 – Configures level 2 routing</li></ul>                                     |
| mode [active standby] | Optional. Configures the cluster mode <ul style="list-style-type: none"><li>• active – Configures this cluster as active</li><li>• standby – Configures this cluster to be on standby mode</li></ul> |

## Usage Guidelines

To add a device to an existing cluster:

- Configure a static IP address on the device (access point, wireless controller, or service platform).
- Provide username and password for superuser, network admin, system admin, or operator accounts.

After adding a device to a cluster, execute the "write memory" command to ensure the configuration persists across reboots.

## Examples (User Exec Mode)

```
rfs4000-229D58>join-cluster 192.168.13.15 user admin password superuser level 1
mode standby
... connecting to 192.168.13.15
... applying cluster configuration
... committing the changes
... saving the changes
[OK]
rfs4000-229D58>
rfs4000-229D58>show context
!
! Configuration of RFS4000 version 5.9.2.0-012D
!
!
version 2.5
!
!
.....
cluster name TechPubs
cluster mode standby
cluster member ip 192.168.13.15 level 1
logging on
logging console warnings
logging buffered warnings
!
!
```

```
end
rfs4000-229D58>
```

### Example (Priv Exec Mode)

```
rfs4000-6DB5D4#join-cluster 192.168.13.16 user admin password superuser level 1
mode standby
... connecting to 192.168.13.16
... applying cluster configuration
... committing the changes
... saving the changes
[OK]
rfs4000-6DB5D4#
rfs4000-6DB5D4#show context
!
! Configuration of RFS6000 version 5.9.2.0-012D

!
!
version 2.5
!
!
.....
cluster name TechPubs
cluster mode standby
cluster member ip 192.168.13.16 level 1
logging on
logging console warnings
logging buffered warnings
!
!
end
rfs4000-6DB5D4#
```

### Related Commands

|                                                                       |                                                                                                                                             |
|-----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">create-cluster (user and privi exec modes)</a> on page 47 | Creates a new cluster on the specified device                                                                                               |
| <a href="#">cluster (user and privi exec modes)</a> on page 46        | Initiates cluster context. The cluster context enables centralized management and configuration of all cluster members from any one member. |

### *l2tpv3 (user and privi exec modes)*

Establishes or brings down a *Layer 2 Tunnel Protocol Version 3* (L2TPV3) tunnel



#### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
l2tpv3 tunnel [<TUNNEL-NAME>|all]
l2tpv3 tunnel <TUNNEL-NAME> [down|session|up]
l2tpv3 tunnel <TUNNEL-NAME> [down|up] {on <DEVICE-NAME>}
l2tpv3 tunnel <TUNNEL-NAME> session <SESSION-NAME> [down|up] {on <DEVICE-NAME>}
l2tpv3 tunnel all [down|up] {on <DEVICE-NAME>}
```

## Parameters

```
l2tpv3 tunnel <TUNNEL-NAME> [down|up] {on <DEVICE-NAME>}
```

|                         |                                                                                                                                                                                                                 |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| l2tpv3 tunnel           | Establishes or brings down L2TPV3 tunnels                                                                                                                                                                       |
| <TUNNEL-NAME> [down up] | Specifies the tunnel name to establish or bring down <ul style="list-style-type: none"><li>down - Brings down the specified tunnel</li><li>up - Establishes the specified tunnel</li></ul>                      |
| on <DEVICE-NAME>        | Optional. Establishes or brings down a tunnel on a specified device <ul style="list-style-type: none"><li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li></ul> |

```
l2tpv3 tunnel <TUNNEL-NAME> session <SESSION-NAME> [down|up] {on <DEVICE-NAME>}
```

|                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| l2tpv3 tunnel                                    | Establishes or brings down L2TPV3 tunnels                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <TUNNEL-NAME> [session <SESSION-NAME>] [down up] | Establishes or brings down a specified session inside an L2TPV3 tunnel <ul style="list-style-type: none"><li>&lt;TUNNEL-NAME&gt; - Specify the tunnel name.</li><li>session &lt;SESSION-NAME&gt; - Identifies a specific session<ul style="list-style-type: none"><li>&lt;SESSION-NAME&gt; - Specify the session name.</li></ul></li><li>down - Brings down the session identified by the &lt;SESSION-NAME&gt; keyword</li><li>up - Establishes the session identified by the &lt;SESSION-NAME&gt; keyword</li></ul> |
| on <DEVICE-NAME>                                 | Optional. Establishes or brings down a tunnel session on a specified device <ul style="list-style-type: none"><li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li></ul>                                                                                                                                                                                                                                                                                              |

```
l2tpv3 tunnel all [down|up] {on <DEVICE-NAME>}
```

|                  |                                                                                                                                                                                                                    |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| l2tpv3 tunnel    | Establishes or brings down L2TPV3 tunnel                                                                                                                                                                           |
| all [down up]    | Establishes or brings down all L2TPV3 tunnels <ul style="list-style-type: none"><li>down - Brings down all tunnels</li><li>up - Establishes all tunnels</li></ul>                                                  |
| on <DEVICE-NAME> | Optional. Establishes or brings down all tunnels on a specified device <ul style="list-style-type: none"><li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li></ul> |

## Examples (User Exec Mode)

```
nx9500-6C8809>l2tpv3 tunnel Tunnel1 session Tunnel1Session1 up on nx9500-6C8809
```

### Example (Privi Exec Mode)

```
nx9500-6C8809#l2tpv3 tunnel TestTunnel session TestTunnelSession1 up on rfs4000-6DB5D4
```



#### Note

For more information on the L2TPV3 tunnel configuration mode and commands, see [L2TPV3-POLICY](#).

### logging (user and privi exec modes)

Modifies message logging settings



#### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
logging monitor {<0-7>/alerts/critical/debugging/emergencies/errors/informational/notifications/warnings}
```

### Parameters

```
logging monitor {<0-7>/alerts/critical/debugging/emergencies/errors/informational/notifications/warnings}
```

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>monitor Sets the terminal lines logging levels. The logging severity levels can be set from 0 - 7. The system configures default settings, if no logging severity level is specified.</p> <ul style="list-style-type: none"><li>• &lt;0-7&gt; - Optional. Specify the logging severity level from 0-7. The various levels and their implications are as follows:</li><li>• alerts - Optional. Immediate action needed (severity=1)</li><li>• critical - Optional. Critical conditions (severity=2)</li><li>• debugging - Optional. Debugging messages (severity=7)</li><li>• emergencies - Optional. System is unusable (severity=0)</li><li>• errors - Optional. Error conditions (severity=3)</li><li>• informational - Optional. Informational messages (severity=6)</li><li>• notifications - Optional. Normal but significant conditions (severity=5)</li><li>• warnings - Optional. Warning conditions (severity=4)</li></ul> <p><b>Note:</b> Before configuring the message logging level, ensure logging module is enabled. To enable message logging, in the device's configuration mode, execute the logging &gt; on command. Message logging can also be enabled on a profile. All devices using the profile will have message logging enabled.</p> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Example (User Exec Mode)

```
NOC-NX9500(config-device-B4-C7-99-6C-88-09)#logging on
NOC-NX9500>logging monitor debugging
NOC-NX9500>show logging
```

```
Logging module: enabled
 Aggregation time: disabled
 Console logging: level debugging
 Monitor logging: level debugging
 Buffered logging: level warnings
 Syslog logging: level warnings
 Facility: local7
```

Log Buffer (2208029 bytes):

```
Jan 03 06:48:40 2018: NOC-NX9500 : %NSM-4-IFUP: Interface gel is up
Jan 03 06:48:39 2018: NOC-NX9500 : %NSM-4-IFUP: Interface gel is up
Jan 03 06:48:37 2018: NOC-NX9500 : %NSM-4-IFDOWN: Interface gel is down
Jan 03 06:48:36 2018: NOC-NX9500 : %NSM-4-IFUP: Interface gel is up
Jan 02 03:41:56 2018: NOC-NX9500 : %NSM-4-IFUP: Interface ge3 is up
Jan 02 03:41:55 2018: NOC-NX9500 : %NSM-4-IFUP: Interface ge3 is up
Jan 02 03:41:53 2018: NOC-NX9500 : %NSM-4-IFDOWN: Interface ge3 is down
Jan 02 03:41:22 2018: NOC-NX9500 : %NSM-4-IFUP: Interface ge3 is up
Jan 02 03:41:20 2018: NOC-NX9500 : %NSM-4-IFUP: Interface ge3 is up
```

```
--More--
NOC-NX9500>
```

### Example (Priv Exec Mode)

```
nx9500-6C8809#logging monitor warnings
nx9500-6C8809#
rfs4000-229D58#logging monitor 2
rfs4000-229D58#
```

### Related Commands

|                                                 |                                      |
|-------------------------------------------------|--------------------------------------|
| <a href="#">no (user exec mode)</a> on page 83  | Resets terminal lines logging levels |
| <a href="#">no (priv-exec-mode)</a> on page 189 |                                      |

*mint* (user and privi exec modes)

Uses MiNT protocol to perform a ping and trace route to a remote device



#### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
mint [ping|traceroute]
mint ping <MINT-ID> {(count <1-10000>/size <1-64000>/timeout <1-10>)}
mint traceroute <MINT-ID> {(destination-port <1-65535>/max-hops <1-255>/
source-port <1-65535>/timeout <1-255>)}
```

## Parameters

```
mint ping <MINT-ID> {(count <1-10000>/size <1-64000>/timeout <1-10>)}
```

|                 |                                                                                                                                                                                                   |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ping <MINT-ID>  | Sends a MiNT echo message to a specified destination <ul style="list-style-type: none"><li>&lt;MINT-ID&gt; - Specify the destination device's MiNT ID.</li></ul>                                  |
| count <1-10000> | Optional. Sets the number of ping packets sent to the specified MiNT destination <ul style="list-style-type: none"><li>&lt;1-60&gt; - Specify a value from 1 - 10000. The default is 3.</li></ul> |
| size <1-64000>  | Optional. Sets the MiNT payload size in bytes <ul style="list-style-type: none"><li>&lt;1-64000&gt; - Specify a value from 1 - 64000. The default is 64 bytes.</li></ul>                          |
| timeout <1-10>  | Optional. Sets a response time in seconds <ul style="list-style-type: none"><li>&lt;1-10&gt; - Specify a value from 1 sec - 10 sec. The default is 1 second.</li></ul>                            |

```
mint traceroute <MINT-ID> {(destination-port <1-65535>/max-hops <1-255>/
source-port <1-65535>/timeout <1-255>)}
```

|                            |                                                                                                                                                                                                                   |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| traceroute <MINT-ID>       | Prints the route packets trace to a device <ul style="list-style-type: none"><li>&lt;MINT-ID&gt; - Specify the destination device's MiNT ID.</li></ul>                                                            |
| destination-port <1-65535> | Optional. Sets the <i>Equal-cost Multi-path</i> (ECMP) routing destination port <ul style="list-style-type: none"><li>&lt;1-65535&gt; - Specify a value from 1 - 65535. The default port is 45.</li></ul>         |
| max-hops <1-255>           | Optional. Sets the maximum number of hops a traceroute packet traverses in the forward direction <ul style="list-style-type: none"><li>&lt;1-255&gt; - Specify a value from 1 - 255. The default is 30.</li></ul> |
| source-port <1-65535>      | Optional. Sets the ECMP source port <ul style="list-style-type: none"><li>&lt;1-65535&gt; - Specify a value from 1 - 65535. The default port is 45.</li></ul>                                                     |
| timeout <1-255>            | Optional. Sets the minimum response time period in seconds <ul style="list-style-type: none"><li>&lt;1-65535&gt; - Specify a value from 1 sec - 255 sec. The default is 30 seconds.</li></ul>                     |

## Example (User Exec Mode)

```
NOC-NX9500>mint ping 4D.83.30.A4
MiNT ping 4D.83.30.A4 with 64 bytes of data.
Response from 4D.83.30.A4: id=16777216 time=0.262 ms
Response from 4D.83.30.A4: id=33554432 time=2.025 ms
Response from 4D.83.30.A4: id=50331648 time=0.256 ms

--- 4D.83.30.A4 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.256/0.848/2.025 ms
NOC-NX9500>
```

## Example (Privi Exec Mode)

```
rfs4000-229D58#mint ping 68.88.0D.A7
MiNT ping 68.88.0D.A7 with 64 bytes of data.
```

```
Response from 68.88.0D.A7: id=1 time=0.364 ms
Response from 68.88.0D.A7: id=2 time=0.333 ms
Response from 68.88.0D.A7: id=3 time=0.368 ms
```

```
--- 68.88.0D.A7 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.333/0.355/0.368 ms
rfs4000-229D58#
```

## *mkdir*

Creates a new directory in the file system

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
mkdir <DIR>
```

### Parameters

```
mkdir <DIR>
```

<DIR> Specify a directory name.

**Note:** A directory, specified by the <DIR> parameter, is created within the file system.

### Examples

```
rfs4000-229D58#dir
Directory of flash:/.
```

```
drwx Tue Sep 27 06:25:15 2016 log
drwx Sat Jan 1 05:30:08 2000 configs
drwx Sat Jan 1 05:30:08 2000 cache
drwx Wed Nov 4 16:12:15 2015 crashinfo
drwx Mon Sep 26 10:45:03 2016 archived_logs
drwx Sat Jan 1 05:30:08 2000 upgrade
drwx Sat Jan 1 05:30:23 2000 hotspot
drwx Sat Jan 1 05:30:08 2000 floorplans
drwx Sat Jan 1 05:30:08 2000 tmptpd
```

```
rfs4000-229D58#
rfs4000-229D58#mkdir test
rfs4000-229D58#
rfs4000-229D58#dir
Directory of flash:/.
```

```
drwx Tue Sep 27 06:25:15 2016 log
drwx Tue Sep 27 15:20:01 2016 test
drwx Sat Jan 1 05:30:08 2000 configs
drwx Sat Jan 1 05:30:08 2000 cache
drwx Wed Nov 4 16:12:15 2015 crashinfo
drwx Mon Sep 26 10:45:03 2016 archived_logs
drwx Sat Jan 1 05:30:08 2000 upgrade
drwx Sat Jan 1 05:30:23 2000 hotspot
drwx Sat Jan 1 05:30:08 2000 floorplans
```



```
drwx Sat Jan 1 05:30:08 2000 tmptpd
rfs4000-229D58#
```

*more*

Displays files on the device's file system. This command navigates and displays specific files in the device's file system.

The more command also displays the startup configuration file.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
more <FILE>
```

### Parameters

```
more <FILE>
```

|                                                                                   |
|-----------------------------------------------------------------------------------|
| <FILE> Specify the file name and location. Provide the complete path to the file. |
|-----------------------------------------------------------------------------------|

### Examples

```
NOC-NX9500#more flash:/archived_logs/startup.1.log
Jan 23 09:51:23 2017: %KERN-6-INFO: PACE(22 - DEFRAG) : memory = 2064375.
Jan 23 09:51:23 2017: %KERN-6-INFO: PACE(22) : Enabled midstream protocol detection.
Jan 23 09:51:23 2017: %KERN-6-INFO: PACE(23) : Enabled rtp performance measurement.
Jan 23 09:51:23 2017: %KERN-6-INFO: PACE(23) : Enabled metadata dissectors.
Jan 23 09:51:23 2017: %KERN-6-INFO: PACE(23 - DEFRAG) : memory = 2064375.
Jan 23 09:51:23 2017: %KERN-6-INFO: PACE(23) : Enabled midstream protocol detection.
Jan 23 09:51:23 2017: %KERN-6-INFO: PACE(0 - FLOW) : real_sizeof_flow_data = 533
, real_sizeof_flow_data_aligned = 536, sizeof_flow_data = 584, num_flows = 68812,
conn_toh_size = 47893152.
Jan 23 09:51:23 2017: %KERN-6-INFO: PACE(0 - SUBSCRIBER) : real_sizeof_id_data =
992, real_sizeof_id_data_aligned = 992, sizeof_id_data = 996, num_subscribers = 6826,
id_toh_size = 7399384.
--More--
NOC-NX9500#
```

*no (priv-exec-mode)*

Use the no command to revert to turn off an enabled feature or to revert a setting to default value.

The no commands have their own set of parameters that can be reset. These parameters depend on the context in which the command is being used.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
[adoption|captive-portal|cpe|crypto|debug|logging|page|raid|service|terminal|upgrade|virtual-machine|wireless]
no adoption {on <DEVICE-OR-DOMAIN-NAME>}
```

### Note



The **no > adoption** command resets the adoption state of a specified device (and all devices adopted to it) or devices within a specified RF Domain. When executed without specifying the device or RF Domain, the command resets the adoption state of the logged device and all devices, if any, adopted to it.

```
no captive-portal client [captive-portal <CAPTIVE-PORTAL-NAME>|mac <MAC>] {on <DEVICE-OR-DOMAIN-NAME>}
no crypto pki [server|trustpoint]
no crypto pki [server|trustpoint] <TRUSTPOINT-NAME> {del-key {on <DEVICE-NAME>}}|on <DEVICE-NAME>}
no logging monitor
no page
no service [block-adopter-config-update|locator|snmp|ssm|wireless]
no service block-adopter-config-update
no service locator {on <DEVICE-NAME>}
no service snmp sysoid wing5
no service ssm trace pattern {<WORD>} {(on <DEVICE-NAME>)}
no service wireless [trace pattern {<WORD>} {(on <DEVICE-NAME>)}|unsanctioned ap air-terminate <BSSID>
{on <DOMAIN-NAME>}]
no terminal [length|width]
no upgrade <PATCH-NAME> {on <DEVICE-NAME>}
no wireless client [all|<MAC>]
no wireless client all {filter/on}
no wireless client all {filter [wlan <WLAN-NAME>]}
no wireless client all {on <DEVICE-OR-DOMAIN-NAME>} {filter [wlan <WLAN-NAME>]}
no wireless client mac <MAC> {on <DEVICE-OR-DOMAIN-NAME>}
```

The following command is available only on the NX 95XX and NX 96XX series service platforms:

```
no cpe led cpe [<1-24>|all] {on <T5-DEVICE-NAME>}
no virtual-machine assign-usb-ports {on <DEVICE-NAME>}
no raid locate
```

### Parameters

```
no <PARAMETERS>
```

|                 |                                                           |
|-----------------|-----------------------------------------------------------|
| no <PARAMETERS> | Resets or reverts settings based on the parameters passed |
|-----------------|-----------------------------------------------------------|

### Usage Guidelines

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

### Examples

```
NOC-NX9500#no adoption on ?
DEVICE-OR-DOMAIN-NAME AP/Controller/RF-Domain name

NOC-NX9500#
NOC-NX9500#no page
NOC-NX9500#
NOC-NX9500#no upgrade ?
WORD Name of the patch to remove
```

NOC-NX9500#

on (user and privi exec modes)

Executes the following commands in the RF Domain context: *clrscr*, *do*, *end*, *exit*, *help*, *service*, and *show*

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
on rf-domain [<RF-DOMAIN-NAME>|all]
```

### Parameters

```
on rf-domain [<RF-DOMAIN-NAME>|all]
```

|                                     |                                                                                                                                                                                          |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| on rf-domain [<RF-DOMAIN-NAME> all] | Enters the RF Domain context based on the parameter specified                                                                                                                            |
|                                     | <ul style="list-style-type: none"><li>• &lt;RF-DOMAIN-NAME&gt; - Specify the RF Domain name. Enters the specified RF Domain context.</li><li>• all - Specifies all RF Domains.</li></ul> |

### Example (User Exec Mode)

```
nx9500-6C8809>on rf-domain TechPubs
nx9500-6C8809(TechPubs)>?
on RF-Domain Mode commands:

 clrscr Clears the display screen
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 service Service Commands
 show Show running system information

nx9500-6C8809(TechPubs)>
nx9500-6C8809(rf-domain-all)>?
on RF-Domain Mode commands:

 clrscr Clears the display screen
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 service Service Commands
 show Show running system information

nx9500-6C8809(rf-domain-all)>
```

### Example (Privi Exec Mode)

```
nx9500-6C8809#on rf-domain TechPubs
nx9500-6C8809(TechPubs)#
NOC-NX9500#on rf-domain default
NOC-NX9500(default)#?
on RF-Domain Mode commands:
```

```
 clrscr Clears the display screen
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 service Service Commands
 show Show running system information
```

```
NOC-NX9500(default)#
```

```
NOC-NX9500(default)#show sessions on RFS6K-SITE1-VLAN20
```

| INDEX | COOKIE | NAME  | START TIME          | FROM      | ROLE      |
|-------|--------|-------|---------------------|-----------|-----------|
| 1     | 10     | admin | 2018-01-02 04:31:41 | Console   | superuser |
| 2     | 3      | snmp  | 2018-01-02 03:39:59 | 127.0.0.1 | superuser |
| 3     | 4      | snmp2 | 2018-01-02 03:39:59 | 127.0.0.1 | superuser |

```
NOC-NX9500(default)#
```

#### *opendns (user and privi exec modes)*

Fetches the OpenDNS device\_id from the OpenDNS site. Use this command to fetch the OpenDNS device\_id. Once fetched, apply the device\_id to WLANs that are to be OpenDNS enabled.

OpenDNS is a free DNS service that enables swift Web navigation without frequent outages. It is a reliable DNS service that provides the following services: DNS query resolution, Web-filtering, protection against virus and malware attacks, performance enhancement, etc.

This command is part of a set of configurations that are required to integrate WiNG devices with OpenDNS. When integrated, DNS queries going out of the WiNG device (access point, controller, or service platform) are re-directed to OpenDNS (208.67.220.220 or 208.67.222.222) resolvers that act as proxy DNS servers.

For more information on integrating WiNG devices with OpenDNS site, see [Example: Enabling OpenDNS Support](#) on page 194.



#### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
opendns [APIToken|username]
opendns APIToken <OPENDNS-APITOKEN>
opendns username <USERNAME> password <OPENDNS-PSWD> label <LABEL>
```



### Note

Note, as per the current implementation both of the above commands can be used to fetch the device\_id from the OpenDNS site.

## Parameters

```
opendns APIToken <OPENDNS-APITOKEN>
```

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| opendns                     | Fetches the device_id from the OpenDNS site using the OpenDNS API token                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| APIToken <OPENDNS-APITOKEN> | Configures the OpenDNS APIToken. This is the token provided you by CISCO at the time of subscribing for their OpenDNS service. <ul style="list-style-type: none"><li>&lt;OPENDNS-APITOKEN&gt; - Provide the OpenDNS API token (should be a valid token).</li></ul> For every valid OpenDNS API token provided a device_id is returned. Apply this device_id to WLANs that are to be OpenDNS enabled. Once applied, DNS queries originating from associating clients are appended with an additional 31 bytes of data (representing the device ID) at the end of the DNS packet. For information on configuring the device_id in the WLAN context, see <a href="#">opendns</a> on page 586. |

```
opendns username <USERNAME> password <OPENDNS-PSWD> label <LABEL>
```

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| opendns                 | Fetches the device_id from the OpenDNS site using the OpenDNS credentials                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| username <USERNAME>     | Configures the OpenDNS user name. This is your OpenDNS email ID provided by CISCO at the time of subscribing for their OpenDNS service. <ul style="list-style-type: none"><li>&lt;USERNAME&gt; - Provide the OpenDNS user name (should be a valid OpenDNS username).</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| password <OPENDNS-PSWD> | Configures the password associated with the user name specified in the previous step. <ul style="list-style-type: none"><li>&lt;OPENDNS-PSWD&gt; - Provide the OpenDNS password (should be a valid OpenDNS password).</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| label <LABEL>           | Configures the network label. This the label (the user friendly name) of your network, and should be the same as the label (name) configured on the OpenDNS portal. <ul style="list-style-type: none"><li>&lt;LABEL&gt; - Specify your network label.</li></ul> For every set of user name, password, and label passed only one unique device_id is returned. Apply this device_id to WLANs that are to be OpenDNS enabled. Once applied, DNS queries originating from associating clients are appended with an additional 31 bytes of data (representing the device ID) at the end of the DNS packet. For information on configuring the device_id in the WLAN context, see <a href="#">opendns</a> on page 586. |

## Usage Guidelines

Use your OpenDNS credentials to logon to the opendns.org site and use the labels, edit settings, and customize content filtering options to configure Web filtering settings.

## Example

```
ap7161-E6D512>opendns username bob@examplecompany.com password opendns label company_name
Connecting to OpenDNS server...
```

```
device_id = 0014AADF8EDC6C59
ap7161-E6D512>
nx9600-7F3C7F>opendns ApiToken 9110B39543DEB2ECA1F473AE03E8899C00019073 device_id =
001480fe36dcb245
nx9600-7F3C7F>
```

### Example: Enabling OpenDNS Support

The following example shows how to enable OpenDNS support:

- 1 Fetch the OpenDNS device\_id from the OpenDNS site.
  - a In the User/Privilege executable mode execute one of the following commands:

```
nx9500-6C8809#opendns APIToken <OPENDNS-APITOKEN>
nx9500-6C8809#opendns ApiToken 9110B39543DEB2ECA1F473AE03E8899C00019073
device_id = 001480fe36dcb245nx9500-6C8809#
```

OR

```
nx9500-6C8809#opendns username <USERNAME> password <OPENDNS-PSWD> label <LABEL>
```



#### Note

The *OpenDNS API token* and/or *user account credentials* are provided the OpenDNS service provider when subscribing for the OpenDNS service.

- b Apply the device\_id fetched in the step 1 to the WLAN.

```
nx9500-6C8809(config-wlan-opendns)#opendns device-id <OPENDNS-DEVICE-ID>
nx9500-6C8809(config-wlan-opendns)#opendns device-id 001480fe36dcb245
nx9500-6C8809(config-wlan-opendns)#show context
wlan opendns
 ssid opendns
 bridging-mode local
 encryption-type none
 authentication-type none
 opendns device-id 001480fe36dcb245
nx9500-6C8809(config-wlan-opendns)#
```



#### Note

Once applied, DNS queries originating from wireless clients associating with the WLAN are appended with an additional 31 bytes of data (representing the device ID) at the end of the DNS packet.

- 2 Configure a DHCP server policy, and set the DHCP pool's DNS server configuration to point to the OpenDNS servers.

```
nx9500-6C8809(config-dhcp-policy-opendns-pool-opendnsPool)#dns-server 208.67.222.222
```



#### Note

You can configure any one of the following OpenDNS servers: 208.67.222.222 OR 208.67.222.220

```
nx9500-6C8809(config-dhcp-policy-opendns-pool-opendnsPool)#show context
dhcp-pool opendnsPool
 dns-server 208.67.222.222
nx9500-6C8809(config-dhcp-policy-opendns-pool-opendnsPool)#
```

- 3 Apply the DHCP server policy configured in step 2 on the access point, controller, or service platform.

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#use dhcp-server-policy opendns
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context include-factory | include
use
 use profile default-nx9000
 use rf-domain TechPubs
```

```
use database-policy default
use nsight-policy noc
use dhcp-server-policy.opendns
use auto-provisioning-policy TechPubs
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```



#### Note

When configured, DNS queries are forwarded by the access point, controller, or service platform to the specified OpenDNS resolver.

- 4 Configure an IP Access Control List with the following permit and deny rules:

```
nx9500-6C8809(config-ip-acl-OpenDNS)#permit udp any host 208.67.222.222 eq dns rule-
precedence 1 rule-description "allow dns queries only to OpenDNS"
nx9500-6C8809(config-ip-acl-OpenDNS)#deny udp any any eq dns rule-precedence 10 rule-
description "block all DNS queries"
nx9500-6C8809(config-ip-acl-OpenDNS)#permit ip any any rule-precedence 100 rule-
description "allow all other ip packets"
nx9500-6C8809(config-ip-acl-OpenDNS)#show context
ip access-list OpenDNS
permit udp any host 208.67.222.222 eq dns rule-precedence 1 rule-description "allow dns
queries only to OpenDNS"
deny udp any any eq dns rule-precedence 10 rule-description "block all dns queries"
permit ip any any rule-precedence 100 rule-description "allow all other ip packets"
nx9500-6C8809(config-ip-acl-OpenDNS)#
```



#### Note

When configured and applied in the WLAN context, the IP ACL prevents wireless clients from adding their own DNS servers to bypass the Web filtering and network policies enforced by OpenDNS.

- 5 Apply the IP ACL configured in step 4 in the WLAN context.

```
nx9500-6C8809(config-wlan-opendns)#use ip-access-list out OpenDNS
nx9500-6C8809(config-wlan-opendns)#show context
wlan opendns
 ssid opendns
 vlan 1
 bridging-mode local
 encryption-type none
 authentication-type none
 use ip-access-list in OpenDNS
 use ip-access-list out OpenDNS
 opendns device-id 0014AADF8EDC6C59
nx9500-6C8809(config-wlan-opendns)#
```



#### Note

When applied to the WLAN, only the DNS queries directed to the OpenDNS server are forwarded. All other DNS queries are dropped.

*page (user and privi exec modes)*

Toggles a device's paging function. Enabling this option displays the CLI command output page by page, instead of running the entire output at once.



#### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

---

**Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

**Syntax**

page

**Parameters**

None

**Examples (User Exec Mode)**

```
rfs4000-6DB5D4#page
rfs4000-6DB5D4#
```

**Example (Privi Exec Mode)**

```
nx9500-6C8809#page
nx9500-6C8809#
```

**Related Commands**

`no (user exec mode) on` Disables paging  
page 83

`no (priv-exec-mode) on` Disables paging  
page 189

*ping (user and privi exec modes)*

Sends ICMP (Internet Controller Message Protocol) echo messages to a user-specified location

**Note**

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

**Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

**Syntax**

```
ping <IP/HOSTNAME> {count <1-10000>/dont-fragment {count/size}/size <1-64000>/
source [<IP>/pppoe/vlan <1-4094>/wwan]}
```

**Parameters**

```
ping <IP/HOSTNAME> {count <1-10000>/dont-fragment {count/size}/size <1-64000>/
source [<IP>/pppoe/vlan <1-4094>/wwan]}
```



|                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IP/HOSTNAME>                          | Specify the destination IP address or hostname. When entered without any parameters, this command prompts for an IP address or a hostname.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| count <1-10000>                        | Optional. Sets the pings to the specified destination <ul style="list-style-type: none"> <li>&lt;1-10000&gt; – Specify a value from 1 - 10000. The default is 5.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                         |
| dont-fragment {count size}             | Optional. Sets the don't fragment bit in the ping packet. Packets with the dont-fragment bit specified are not fragmented. When a packet, with the dont-fragment bit specified, exceeds the specified MTU (maximum transmission unit) value, an error message is sent from the device trying to fragment it. <ul style="list-style-type: none"> <li>count &lt;1-10000&gt; – Optional. Sets the pings to the specified destination from 1 - 10000. The default is 5.</li> <li>size &lt;1-64000&gt; – Optional. Sets the ping payload size from 1 - 64000 bytes. The default is 100 bytes.</li> </ul> |
| size <1-64000>                         | Optional. Sets the ping payload size in bytes <ul style="list-style-type: none"> <li>&lt;1-64000&gt; – Specify the ping payload size from 1 - 64000. The default is 100 bytes.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                           |
| source [<IP> pppoe vlan <1-4094> wwan] | Optional. Sets the source address or interface name. This is the source of the ICMP packet to the specified destination. <ul style="list-style-type: none"> <li>&lt;IP&gt; – Specifies the source IP address</li> <li>pppoe – Selects the PPP over Ethernet interface</li> <li>vlan &lt;1-4094&gt; – Selects the VLAN interface from 1 - 4094</li> <li>wwan – Selects the wireless WAN interface</li> </ul>                                                                                                                                                                                         |

### Examples (User Exec Mode)

```
NOC-NX9500>ping 10.234.160.13
PING 10.234.160.13 (10.234.160.13) 100(128) bytes of data.
108 bytes from 10.234.160.13: icmp_seq=1 ttl=64 time=3.61 ms
108 bytes from 10.234.160.13: icmp_seq=2 ttl=64 time=0.177 ms
108 bytes from 10.234.160.13: icmp_seq=3 ttl=64 time=0.162 ms
108 bytes from 10.234.160.13: icmp_seq=4 ttl=64 time=0.167 ms
108 bytes from 10.234.160.13: icmp_seq=5 ttl=64 time=0.170 ms

--- 10.234.160.13 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.162/0.857/3.613/1.378 ms
NOC-NX9500>
NOC-NX9500>ping 10.234.160.11 source vlan 1
PING 10.234.160.11 (10.234.160.11) from 10.234.160.5 vlan1: 100(128) bytes of data.
108 bytes from 10.234.160.11: icmp_seq=1 ttl=64 time=6.87 ms
108 bytes from 10.234.160.11: icmp_seq=2 ttl=64 time=0.469 ms
108 bytes from 10.234.160.11: icmp_seq=3 ttl=64 time=0.448 ms
108 bytes from 10.234.160.11: icmp_seq=4 ttl=64 time=0.437 ms
108 bytes from 10.234.160.11: icmp_seq=5 ttl=64 time=0.459 ms

--- 10.234.160.11 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
rtt min/avg/max/mdev = 0.437/1.738/6.879/2.570 ms
NOC-NX9500>
```

### Examples (Privi Exec Mode)

```
rfs4000-229D58#ping 10.233.89.182 source vlan 1
PING 10.233.89.182 (10.233.89.182) from 192.168.13.24 vlan1: 100(128) bytes of data.
From 192.168.13.2 icmp_seq=1 Packet filtered
From 192.168.13.2 icmp_seq=2 Packet filtered
From 192.168.13.2 icmp_seq=3 Packet filtered
```

```

From 192.168.13.2 icmp_seq=4 Packet filtered
From 192.168.13.2 icmp_seq=5 Packet filtered

--- 10.233.89.182 ping statistics ---
5 packets transmitted, 0 received, +5 errors, 100% packet loss, time 3997ms

rfs4000-229D58#

```

### ping6 (user and privi exec modes)

Sends ICMPv6 echo messages to a user-specified IPv6 address



#### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
ping6 <IPv6/HOSTNAME> {<INTF-NAME>} {(count <1-10000>|size <1-64000>)}
```

### Parameters

```
ping6 <IPv6/HOSTNAME> {<INTF-NAME>} {(count <1-10000>|size <1-64000>)}
```

|                 |                                                                                                                                                                                                  |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IPv6/HOSTNAME> | Specify the destination IPv6 address or hostname.                                                                                                                                                |
| <INTF-NAME>     | Specify the interface name for link local/broadcast address                                                                                                                                      |
| count <1-10000> | Optional. Sets the pings to the specified IPv6 destination <ul style="list-style-type: none"> <li>• &lt;1-10000&gt; - Specify a value from 1 - 10000. The default is 5.</li> </ul>               |
| size <1-64000>  | Optional. Sets the IPv6 ping payload size in bytes <ul style="list-style-type: none"> <li>• &lt;1-64000&gt; - Specify the ping payload size from 1 - 64000. The default is 100 bytes.</li> </ul> |

### Usage Guidelines

To configure a device's IPv6 address, in the VLAN interface configuration mode, use the **ipv6 > address <IPv6-ADDRESS>** command. After configuring the IPv6 address, use the **ipv6 > enable** command to enable IPv6. For more information, see [ipv6](#) on page 1162 (profile config mode).

### Examples (User Exec Mode)

```

rfs4000-1B3596(config-device-00-23-68-1B-35-96-if-ge4)#show ipv6 interface brief

INTERFACE IPV6 MODE IPV6-ADDRESS/MASK TYPE STATUS PROTOCOL

vlan1 True fe80::223:68ff:fe88:da7/64 Link-Local UP up
vlan1 True 2001:10:10:10:10:10:10:1/64 Global-Permanent UP up
vlan2 False UNASSIGNED None UP up

```

```

rfs4000-1B3596(config-device-00-23-68-1B-35-96-if-ge4)#
rfs4000-229D58>ping6 2001:10:10:10:10:10:10:1 count 6
PING 2001:10:10:10:10:10:10:1(2001:10:10:10:10:10:10:1) 100 data bytes
108 bytes from 2001:10:10:10:10:10:10:1: icmp_seq=1 ttl=64 time=0.401 ms
108 bytes from 2001:10:10:10:10:10:10:1: icmp_seq=2 ttl=64 time=0.311 ms
108 bytes from 2001:10:10:10:10:10:10:1: icmp_seq=3 ttl=64 time=0.300 ms
108 bytes from 2001:10:10:10:10:10:10:1: icmp_seq=4 ttl=64 time=0.309 ms
108 bytes from 2001:10:10:10:10:10:10:1: icmp_seq=5 ttl=64 time=0.299 ms
108 bytes from 2001:10:10:10:10:10:10:1: icmp_seq=6 ttl=64 time=0.313 ms

--- 2001:10:10:10:10:10:10:1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 6999ms
rtt min/avg/max/mdev = 0.299/0.318/0.401/0.031 ms
rfs4000-229D58>

```

### Examples (Privi Exec Mode)

```

rfs4000-880DA7#ping6 2001:10:10:10:10:10:10:2 count 6 size 200
PING 2001:10:10:10:10:10:10:2(2001:10:10:10:10:10:10:2) 200 data bytes
208 bytes from 2001:10:10:10:10:10:10:2: icmp_seq=1 ttl=64 time=0.509 ms
208 bytes from 2001:10:10:10:10:10:10:2: icmp_seq=2 ttl=64 time=0.323 ms
208 bytes from 2001:10:10:10:10:10:10:2: icmp_seq=3 ttl=64 time=0.318 ms
208 bytes from 2001:10:10:10:10:10:10:2: icmp_seq=4 ttl=64 time=0.317 ms
208 bytes from 2001:10:10:10:10:10:10:2: icmp_seq=5 ttl=64 time=0.314 ms
208 bytes from 2001:10:10:10:10:10:10:2: icmp_seq=6 ttl=64 time=0.318 ms

--- 2001:10:10:10:10:10:10:2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4999ms
rtt min/avg/max/mdev = 0.314/0.349/0.509/0.075 ms
rfs4000-880DA7#

```

### *pwd*

Displays the full path of the present working directory, similar to the UNIX `pwd` command

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
pwd
```

### Parameters

None

### Examples

```

rfs4000-229D58#pwd
flash:/
rfs4000-229D58#
rfs4000-229D58#dir
Directory of flash:/

```

```

drwx Mon Feb 8 17:37:21 2016 log
drwx Sat Jan 1 05:30:08 2000 configs
drwx Sat Jan 1 05:30:08 2000 cache
drwx Thu Nov 12 17:55:02 2015 crashinfo

```

```

drwx Mon Feb 8 17:34:21 2016 archived_logs
drwx Sat Jan 1 05:30:08 2000 upgrade
drwx Sat Jan 1 05:30:23 2000 hotspot
drwx Sat Jan 1 05:30:08 2000 floorplans
drwx Sat Jan 1 05:30:08 2000 tmpd

```

```
rfs4000-229D58#
```

### re-elect

Re-elects the tunnel controller (wireless controller or service platform)

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
re-elect tunnel-controller {<WORD> {on <DEVICE-NAME>}|on <DEVICE-NAME>}
```

#### Parameters

```
re-elect tunnel-controller {<WORD> {on <DEVICE-NAME>}|on <DEVICE-NAME>}
```

|                            |                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| re-elect tunnel-controller | Re-elects the tunnel controller                                                                                                                                                                                                                                                                                                                                    |
| <WORD> {on <DEVICE-NAME>}  | Optional. Re-elects the tunnel controller on all devices whose preferred tunnel controller name matches <WORD> <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; - Optional. Re-elects the tunnel controller on a specified device</li> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

#### Example

```

rfs4000-229D58#re-elect tunnel-controller
OK
rfs4000-229D58#

```

### reload

Halts a device or devices and performs a warm reboot

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
reload {<DEVICE-MAC-OR-HOSTNAME>|at|cancel|force|in|on|staggered}
reload {(<DEVICE-MAC-OR-HOSTNAME>)}
reload {at <TIME> <1-31> <MONTH> <1993-2035> {on <DEVICE-OR-DOMAIN-NAME>}}
reload {cancel} {on <DEVICE-OR-DOMAIN-NAME>}
reload {force} {(<DEVICE-MAC-OR-HOSTNAME> |on <DOMAIN-NAME> |staggered)}
reload {force} {on <DOMAIN-NAME> {staggered} |staggered {<DEVICE-MAC-OR-HOSTNAME> |
on <DOMAIN-NAME>}} {containing <WORD> |exclude-controllers |exclude-rf-domain-manager |
filter <DEVICE-TYPE>}
reload {in <1-999>} {list|on}
reload {in <1-999>} {list {<LINE>|all} |on <DEVICE-OR-DOMAIN-NAME>}
reload {in <1-999>} {on <DEVICE-OR-DOMAIN-NAME>}
reload {on <DOMAIN-NAME>} {containing <WORD> |exclude-controllers |
exclude-rf-domain-manager |filter <DEVICE-TYPE>}
reload {staggered} {(<DEVICE-MAC-OR-HOSTNAME>) |on <DOMAIN-NAME>} {containing <WORD> |
exclude-controllers |exclude-rf-domain-manager |filter <DEVICE-TYPE>}
```

## Parameters

```
reload {on <DEVICE-OR-DOMAIN-NAME>}
```

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| reload <DEVICE-MAC-OR-HOSTNAME> | <p>Initiates device(s) reload and configures associated parameters</p> <p>The following keyword is recursive and allows you to specify multiple devices:</p> <ul style="list-style-type: none"><li>• &lt;DEVICE-MAC-OR-HOSTNAME&gt; – Optional. Reloads a specified device(s), identified by the &lt;DEVICE-MAC-OR-HOSTNAME&gt; keyword. Specify the device's hostname or MAC address.</li></ul> <p><b>Note:</b> If no device is specified, the system reloads the logged device.</p> |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
reload {at <TIME> <1-31> <MONTH> <1993-2035> {on <DEVICE-OR-DOMAIN-NAME>}}
```

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| reload at                  | <p>Initiates device(s) reload and configures associated parameters</p> <ul style="list-style-type: none"><li>• at – Optional. Schedules a reload at a specified time and day. Use the following keywords to specify the time and day: &lt;TIME&gt;, &lt;1-31&gt;, &lt;MONTH&gt;, and &lt;1993-2035&gt;.</li></ul>                                                                                                                                                                       |
| <TIME>                     | Specifies the time in the HH:MM:SS format                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <1-31>                     | Specifies the day of the month from 1 - 31                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <MONTH>                    | Specifies the month from Jan - Dec                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <1993-2035>                | Specifies the year from 1993 - 2035. It should be a valid 4 digit year.                                                                                                                                                                                                                                                                                                                                                                                                                 |
| on <DEVICE-OR-DOMAIN-NAME> | <p>Optional. Performs reload at the scheduled time, on a specified device or all devices within a specified RF Domain</p> <ul style="list-style-type: none"><li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain. When a RF Domain name is provided, all devices within the specified RF Domain are reloaded at the scheduled time. If no device is specified, the reload is scheduled on the logged device.</li></ul> |

```
reload {cancel} {on <DEVICE-OR-DOMAIN-NAME>}
```

|                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| reload cancel on<br><DEVICE-OR-<br>DOMAIN-NAME> | <p>Cancels pending/scheduled reloads of device(s) cancel – Optional. Cancels all pending reloads</p> <ul style="list-style-type: none"> <li>on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Cancels reloads pending on a specified device or all devices within a specified RF Domain</li> <li>&lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> <p><b>Note:</b> If no device is specified, the system cancels reloads pending on the logged device.</p> |
| on <DEVICE-OR-<br>DOMAIN-NAME>                  | <p>Optional. Reloads on a specified device or RF Domain</p> <ul style="list-style-type: none"> <li>&lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul>                                                                                                                                                                                                                                                                                                  |

```
reload {force} {(<DEVICE-MAC-OR-HOSTNAME>)}
```

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| reload force                 | <p>Initiates device(s) reload and configures associated parameters</p> <ul style="list-style-type: none"> <li>force – Optional. Forces device(s) to reload, while ignoring conditions like upgrade in progress, unsaved changes, etc. Use the options provided to force a reload on a specified device or all devices in a RF Domain.</li> </ul>                                                                                                                                                                  |
| <DEVICE-MAC-OR-<br>HOSTNAME> | <p>This keyword is recursive and allows you to specify multiple devices.</p> <ul style="list-style-type: none"> <li>&lt;DEVICE-MAC-OR-HOSTNAME&gt; – Optional. Forces a reload on a specified device identified by the &lt;DEVICE-MAC-OR-HOSTNAME&gt; keyword. Specify the device's hostname or MAC address. When executed, the specified device(s) are forced to halt and a warm reboot is performed.</li> </ul> <p><b>Note:</b> If no device is specified, the system forcefully reloads the logged device.</p> |

```
reload {force} {on <DOMAIN-NAME> {staggered}/staggered {<DEVICE-MAC-OR-HOSTNAME>/on
<DOMAIN-NAME>}}
{containing <WORD>/exclude-controllers/exclude-rf-domain-manager/filter <DEVICE-TYPE>}
```

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| reload force                  | <p>Initiates device(s) reload and configures associated parameters</p> <ul style="list-style-type: none"> <li>force – Optional. Forces device(s) to reload, while ignoring conditions like upgrade in progress, unsaved changes, etc. Use the options provided to force a reload on a specified device or all devices in a RF Domain.</li> </ul>                                                                                                                                                                                                                                                |
| on <DOMAIN-NAME><br>staggered | <p>Optional. Forces a reload on all devices in a RF Domain</p> <ul style="list-style-type: none"> <li>&lt;DOMAIN-NAME&gt; – Optional. Specify the name of the RF Domain. When executed, all devices within the specified RF Domain are forced to halt and a warm reboot is performed.</li> <li>staggered – Optional. Enables staggered reload of devices (one at a time) without network impact. Use this option when rebooting multiple devices within an RF Domain. When executed, all devices within the specified RF Domain are forced to halt and reboot in a staggered manner.</li> </ul> |

|                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>staggered {&lt;DEVICE-MAC-OR-HOSTNAME&gt;} on &lt;DOMAIN-NAME&gt;}</p>                                    | <p>Optional. Enables staggered reload of devices (one at a time) without network impact</p> <ul style="list-style-type: none"> <li>• &lt;DEVICE-MAC-OR-HOSTNAME&gt; – Optional. Forces a reload on specified device(s) identified by the &lt;DEVICE-MAC-OR-HOSTNAME&gt; keyword. Specify the device’s hostname or MAC address. This is a recursive keyword that allows you to specify multiple devices. When executed, the specified device(s) are forced to halt and a warm reboot is performed.</li> <li>• on &lt;DOMAIN-NAME&gt; – Optional. Forces a reload on all devices in a RF Domain. Specify the name of the RF Domain. When executed, all devices within the specified RF Domain are forced to halt and a warm reboot is performed.</li> </ul> <p><b>Note:</b> If no device or RF Domain is specified, the system forcefully reloads the logged device.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <p>{containing &lt;WORD&gt;} exclude-controllers  exclude-rf-domain-manager  filter &lt;DEVICE-TYPE&gt;}</p> | <p>When forcefully reloading devices in a RF Domain, you can use following options to filter specific devices or device types:</p> <ul style="list-style-type: none"> <li>• containing &lt;WORD&gt; – Optional. Filters out devices containing a specified sub-string in their hostnames <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Optional. Provide the sub-string to match. All devices having hostnames containing the provided sub-string are filtered and forcefully reloaded.</li> </ul> </li> <li>• exclude-controllers – Optional. Excludes all controllers in the specified RF Domain from the reload process</li> <li>• exclude-rf-domain-manager – Optional. Excludes the RF Domain manager from the reload process</li> <li>• filter &lt;DEVICE-TYPE&gt; – Optional. Filters devices by the device type specified. Select the type of device. All devices, of the specified type, within the specified RF Domain, are forcefully reloaded. <ul style="list-style-type: none"> <li>• &lt;DEVICE-TYPE&gt; – Select the type of device to reload. The options are:AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533, RFS 4000, NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000, and t5.</li> </ul> </li> </ul> |

```
reload {in <1-999>} {list {<LINE>|all}|on <DEVICE-OR-DOMAIN-NAME>}
```

|                                         |                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>reload in &lt;1-999&gt;</p>          | <p>Initiates device(s) reload and configures associated parameters</p> <ul style="list-style-type: none"> <li>• in – Optional. Performs a reload after a specified time period <ul style="list-style-type: none"> <li>• &lt;1-999&gt; – Specify the time from 1 - 999 minutes</li> </ul> </li> </ul>     |
| <p>list {&lt;LINE&gt; all}</p>          | <p>Optional. Reloads all adopted devices or specified devices</p> <ul style="list-style-type: none"> <li>• &lt;LINE&gt; – Optional. Reloads listed devices. List all devices (to be reloaded) separated by a space.</li> <li>• all – Optional. Reloads all devices adopted by this controller</li> </ul> |
| <p>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</p> | <p>Optional. Reloads a specified device or all devices within a specified RF Domain</p> <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul>                                             |

```
reload {on <DOMAIN-NAME>} {containing <WORD>|exclude-controllers| exclude-rf-domain-manager|filter <DEVICE-TYPE>}
```

|                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>reload on &lt;DOMAIN-NAME&gt;</p>                                                                         | <p>Initiates device(s) reload and configures associated parameters</p> <ul style="list-style-type: none"> <li>• on &lt;DOMAIN-NAME&gt; - Optional. Enables reload of all devices in a RF Domain</li> <li>• &lt;DOMAIN-NAME&gt; - Specify the name of the RF Domain. When executed, all devices within the specified RF Domain are immediately halted and a warm reboot is performed.</li> </ul> <p><b>Note:</b> If no RF Domain is specified, the system reloads the logged device.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <p>{containing &lt;WORD&gt;  exclude-controllers  exclude-rf-domain-manager  filter &lt;DEVICE-TYPE&gt;}</p> | <p>When reloading devices in a RF Domain, you can use following options to filter specific devices or device types:</p> <ul style="list-style-type: none"> <li>• containing &lt;WORD&gt; - Optional. Filters out devices containing a specified sub-string in their hostnames. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Optional. Provide the sub-string to match. All devices having hostnames containing the provided sub-string are filtered and forcefully reloaded.</li> </ul> </li> <li>• exclude-controllers - Optional. Excludes all controllers in the specified RF Domain from the reload process</li> <li>• exclude-rf-domain-manager - Optional. Excludes the RF Domain manager from the reload process</li> <li>• filter &lt;DEVICE-TYPE&gt; - Optional. Filters devices by the device type specified. Select the type of device to reload. All devices, of the specified type, within the specified RF Domain, are forcefully reloaded. <ul style="list-style-type: none"> <li>• &lt;DEVICE-TYPE&gt; - Select the type of device to reload. The options are: AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533, RFS 4000, NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000, and t5. All devices of the type specified are reloaded.</li> </ul> </li> </ul> |

```
reload {staggered} {(<DEVICE-MAC-OR-HOSTNAME>)|on <DOMAIN-NAME>} {containing <WORD>|
exclude-controllers|exclude-rf-domain-manager|filter <DEVICE-TYPE>}
```



|                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>reload staggered</p> <p>{&lt;DEVICE-MAC-OR-HOSTNAME&gt;  on &lt;DOMAIN-NAME&gt;}</p>                      | <p>Initiates device(s) reload and configures associated parameters</p> <ul style="list-style-type: none"> <li>staggered – Optional. Enables staggered reload of devices (one at a time) without network impact</li> </ul> <p>Use one of the following options to specify a single device, multiple devices, or a RF Domain</p> <ul style="list-style-type: none"> <li>&lt;DEVICE-MAC-OR-HOSTNAME&gt; – Optional. Performs staggered reload on specified device(s) identified by the &lt;DEVICE-MAC-OR-HOSTNAME&gt; keyword. Specify the device’s hostname or MAC address. This is a recursive keyword that allows you to specify multiple devices. When executed, the specified device(s) are halted and a warm reboot is performed. Multiple devices are halted and rebooted one at a time without impacting network functioning.</li> <li>&lt;DOMAIN-NAME&gt; – Optional. Performs staggered reload of all devices in a RF Domain. Specify the name of the RF Domain. When executed, devices in the specified RF Domain are halted and rebooted one at a time without impacting network functioning. Use additional filter options to filter devices in the specified RF Domain.</li> </ul> <p><b>Note:</b> If no device or RF Domain is specified, the system reloads the logged device.</p> |
| <p>{containing &lt;WORD&gt;  exclude-controllers  exclude-rf-domain-manager  filter &lt;DEVICE-TYPE&gt;}</p> | <p>When reloading devices in a RF Domain, you can use following options to filter specific devices or device types:</p> <ul style="list-style-type: none"> <li>containing &lt;WORD&gt; – Optional. Filters out devices containing a specified sub-string in their hostnames. <ul style="list-style-type: none"> <li>&lt;WORD&gt; – Optional. Provide the sub-string to match. All devices having hostnames containing the provided sub-string are filtered and reloaded.</li> </ul> </li> <li>exclude-controllers – Optional. Excludes all controllers in the specified RF Domain from the reload process</li> <li>exclude-rf-domain-manager – Optional. Excludes the RF Domain manager from the reload process</li> <li>filter &lt;DEVICE-TYPE&gt; – Optional. Filters devices by the device type specified. Select the type of device. All devices, of the specified type, within the specified RF Domain, are reloaded. <ul style="list-style-type: none"> <li>&lt;DEVICE-TYPE&gt; – Select the type of device to reload. The options are: AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533, RFS 4000, NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000, and t5.</li> </ul> </li> </ul>                      |

### Example

```

nx9500-6C8809#reload at 12:30:00 10 Jan 2018 on rfs4000-6DB5D4
Reload scheduled at 2018-01-10 12:30:00 UTC ...
nx9500-6C8809#
nx9500-6C8809#reload cancel on rfs4000-6DB5D4
Scheduled reload cancelled.
nx9500-6C8809#

```

### rename

Renames a file in the devices’ file system

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
rename <OLD-FILE-NAME> <NEW-FILE-NAME>
```

### Parameters

```
rename <OLD-FILE-NAME> <NEW-FILE-NAME>
```

|                 |                             |
|-----------------|-----------------------------|
| <OLD-FILE-NAME> | Specify the file to rename. |
| <NEW-FILE-NAME> | Specify the new file name.  |

### Examples

```
rfs4000-229D58#dir
Directory of flash:/.
```

```
drwx Wed Sep 14 13:54:10 2016 log
drwx Sat Jan 1 05:30:08 2000 configs
drwx Sat Jan 1 05:30:08 2000 cache
drwx Wed Nov 4 16:12:15 2015 crashinfo
drwx Fri Sep 16 05:26:37 2016 testdir
drwx Thu Sep 8 04:09:30 2016 archived_logs
drwx Sat Jan 1 05:30:08 2000 upgrade
drwx Sat Jan 1 05:30:23 2000 hotspot
drwx Sat Jan 1 05:30:08 2000 floorplans
drwx Sat Jan 1 05:30:08 2000 tmptpd
```

```
rfs4000-229D58#
rfs4000-229D58#rename flash:/testdir/ Final
rfs4000-229D58#
rfs4000-229D58#dir
Directory of flash:/.
```

```
drwx Wed Sep 14 13:54:10 2016 log
drwx Sat Jan 1 05:30:08 2000 configs
drwx Fri Sep 16 05:26:37 2016 Final
drwx Sat Jan 1 05:30:08 2000 cache
drwx Wed Nov 4 16:12:15 2015 crashinfo
drwx Thu Sep 8 04:09:30 2016 archived_logs
drwx Sat Jan 1 05:30:08 2000 upgrade
drwx Sat Jan 1 05:30:23 2000 hotspot
drwx Sat Jan 1 05:30:08 2000 floorplans
drwx Sat Jan 1 05:30:08 2000 tmptpd
```

```
rfs4000-229D58#
```

### *rmdir*

Deletes an existing directory from the file system (only empty directories can be removed)

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533

- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
rmdir <DIR>
```

### Parameters

```
rmdir <DIR>
```

```
rmdir <DIR> Specifies the directory name
```

**Note:** The directory, specified by the <DIR> parameter, is removed from the file system.

### Examples

```
rfs4000-229D58#dir
Directory of flash:/.
```

```
drwx Wed Sep 14 13:54:10 2016 log
drwx Sat Jan 1 05:30:08 2000 configs
drwx Fri Sep 16 05:26:37 2016 Final
drwx Sat Jan 1 05:30:08 2000 cache
drwx Wed Nov 4 16:12:15 2015 crashinfo
drwx Thu Sep 8 04:09:30 2016 archived_logs
drwx Sat Jan 1 05:30:08 2000 upgrade
drwx Sat Jan 1 05:30:23 2000 hotspot
drwx Sat Jan 1 05:30:08 2000 floorplans
drwx Sat Jan 1 05:30:08 2000 tmptpd
```

```
rfs4000-229D58#
rfs4000-229D58#rmdir Final
rfs4000-229D58#
rfs4000-229D58#dir
Directory of flash:/.
```

```
drwx Wed Sep 14 13:54:10 2016 log
drwx Sat Jan 1 05:30:08 2000 configs
drwx Sat Jan 1 05:30:08 2000 cache
drwx Wed Nov 4 16:12:15 2015 crashinfo
drwx Thu Sep 8 04:09:30 2016 archived_logs
drwx Sat Jan 1 05:30:08 2000 upgrade
drwx Sat Jan 1 05:30:23 2000 hotspot
drwx Sat Jan 1 05:30:08 2000 floorplans
drwx Sat Jan 1 05:30:08 2000 tmptpd
```

```
rfs4000-229D58#
```

*self*

Enters the logged device's configuration context

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

self

## Parameters

None

## Examples

```
nx9500-6C8809#self
Enter configuration commands, one per line. End with CNTL/Z.
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```

*ssh (user and privi exec modes)*

Opens a SSH (Secure Shell) connection between two network devices



### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

## Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
ssh <IP/HOSTNAME> <USER-NAME> {<INF-NAME/LINK-LOCAL-ADD>}
```

## Parameters

```
ssh <IP/HOSTNAME> <USER-NAME> {<INF-NAME/LINK-LOCAL-ADD>}
```

|                            |                                                                                |
|----------------------------|--------------------------------------------------------------------------------|
| <IP/HOSTNAME>              | Specify the remote system's IP address or hostname.                            |
| <USERNAME>                 | Specify the name of the user requesting SSH connection with the remote system. |
| <INF-NAME/ LINK-LOCAL-ADD> | Optional. Specify the interface's name or link local address.                  |

## Example (User Exec Mode)

```
NOC-NX9500>ssh 10.234.160.13 admin
admin@10.234.160.13's password:
ap8432-070235>>ssh 192.168.13.24 admin
admin@192.168.13.24's password:
rfs4000-6DB5D4>
```

## Example (Privi Exec Mode)

```
ap7532-DF9A4C#ssh 10.234.160.13 admin
admin@10.234.160.13's password:
ap8432-070235>
```

*t5 (privi exec mode)*

Executes following operations on a T5 device through the WiNG controller:

- copy, rename, and delete files on the T5 device's file system
- write running configuration to the T5 device's memory

The T5 switch is a means of providing cost-effective, high-speed, wall-to-wall coverage across a building. The T5 switch leverages the in-building telephone lines to extend Ethernet and Wireless LAN networks without additional expenditure on re-wiring. This setup is ideally suited for hotels, providing high-speed Wi-Fi coverage to guest rooms.

The entire setup consists of the DSL T5 switch, TW-510 Ethernet wallplates, and TW-511 wireless wallplate access points. Replace the phone jack plate in a room with the TW-511 delivers 802.11 a/b/g/n and extend wireless connectivity in that room and the neighboring rooms. These TW-511 wallplates (also referred to as the CPEs) are connected to the T5 switch over the DSL interface using a phone block.

The T5 switch is adopted and managed through a WiNG controller. The connection between the T5 and WiNG switches is over a WebSocket.



#### Note

For more information on other T5 CPE related commands, see [cpe \(privilege-exec-mode\)](#) on page 134.

#### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
t5 [copy <SOURCE-FILE-NAME> <DEST-FILE-NAME>|delete <FILE-NAME>|
rename <SOURCE-FILE-NAME> <DEST-FILE-NAME>|write memory] {on <T5-DEVICE-NAME>}
```

#### Parameters

```
t5 [copy <SOURCE-FILE-NAME> <DEST-FILE-NAME>|delete <FILE-NAME>|
rename <SOURCE-FILE-NAME> <DEST-FILE-NAME>|write memory] {on <T5-DEVICE-NAME>}
```

|                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| copy <SOURCE-FILE-NAME> <DEST-FILE-NAME>   | <p>Copies file to an external server</p> <ul style="list-style-type: none"> <li>• &lt;SOURCE-FILE-NAME&gt; - Specify the source file name.</li> <li>• &lt;DEST-FILE-NAME&gt; - Specify the destination file name.</li> </ul> <p>The content from the source file is copied to the destination file.</p> <p>The source or destination files can be local or remote FTP or TFTP files. The source file also can be a pre-defined keyword. At least one of the files should be a local file. Use this command to copy the startup and/or running configurations to an external server.</p> |
| delete <FILE-NAME>                         | <p>Deletes files on the T5 device's file system</p> <ul style="list-style-type: none"> <li>• &lt;FILE-NAME&gt; - Specify the file name. The specified file is deleted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                       |
| rename <SOURCE-FILE-NAME> <DEST-FILE-NAME> | <p>Renames a file on the T5 device's file system</p> <ul style="list-style-type: none"> <li>• &lt;SOURCE-FILE-NAME&gt; - Specify the source file name</li> <li>• &lt;DEST-FILE-NAME&gt; - Specify the new file name. The source file is renamed to the input provided here.</li> </ul>                                                                                                                                                                                                                                                                                                  |

|                     |                                                                                                                                                                                                    |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| write memory        | Writes running configuration to an adopted T5 device's memory <ul style="list-style-type: none"> <li>memory - Writes running configuration to the T5 device's non-volatile (NV) memory.</li> </ul> |
| on <T5-DEVICE-NAME> | Optional. Executes these operation on a specified T5 device <ul style="list-style-type: none"> <li>&lt;T5-DEVICE-NAME&gt; - Specify the T5 device's hostname.</li> </ul>                           |

### Example

```
nx9500-6C8809#t5 write memory on t5-ED7C6C
Success
nx9500-6C8809#
```

*telnet (user and privi exec modes)*

Opens a Telnet session between two network devices



### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
telnet <IP/HOSTNAME> {<TCP-PORT>} {<INTF-NAME>}
```

### Parameters

```
telnet <IP/HOSTNAME> {<TCP-PORT>} {<INTF-NAME>}
```

|               |                                                                                                                                                                                                                                                                                                                |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IP/HOSTNAME> | Configures the destination remote system's IP (IPv4 or IPv6) address or hostname. The Telnet session is established between the connecting system and the remote system. <ul style="list-style-type: none"> <li>&lt;IP/HOSTNAME&gt; - Specify the remote system's IPv4 or IPv6 address or hostname.</li> </ul> |
| <TCP-PORT>    | Optional. Specify the <i>Transmission Control Protocol</i> (TCP) port number.                                                                                                                                                                                                                                  |
| <INTF-NAME>   | Optional. Specify the interface name for the link local address.                                                                                                                                                                                                                                               |

### Examples (User Exec Mode)

```
NOC-NX9500>telnet 10.234.160.11
telnet: cannot connect to remote host (10.234.160.11): Connection refused
NOC-NX9500>telnet 10.234.160.13
```

```
Entering character mode
Escape character is '^]'.

```

```
AP8432 release 5.9.2.0-029R
ap8432-070235 login:
```

### Example (Privi Exec Mode)

```
NOC-NX9500#telnet 10.234.160.12
```

```
Entering character mode
Escape character is '^]'.
^Z
^_
```

```
AP7532 release 5.9.2.0-029R
ap7532-DF9A4C login:
```

*terminal (user and privi exec modes)*

Sets the length and width of the CLI display window on a terminal



#### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
terminal [length|width] <0-512>
```

### Parameters

```
terminal [length|width] <0-512>
```

|                |                                                                                                                                                                            |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| length <0-512> | Sets the number of lines displayed on a terminal window <ul style="list-style-type: none"><li>• &lt;0-512&gt; - Specify a value from 0 - 512.</li></ul>                    |
| width <0-512>  | Sets the width (the number of characters displayed) of the terminal window <ul style="list-style-type: none"><li>• &lt;0-512&gt; - Specify a value from 0 - 512.</li></ul> |

### Example (User Exec Mode)

```
ap8432-070235>show terminal
Terminal Type: xterm
Length: 24 Width: 80
ap8432-070235>
ap8432-070235>terminal length 80
ap8432-070235>terminal width 100
ap8432-070235>show terminal
Terminal Type: xterm
Length: 80 Width: 100
ap8432-070235>
```

### Example (Privi Exec Mode)

```
NOC-NX9500#show terminal
Terminal Type: xterm
```

```
Length: 24 Width: 80
NOC-NX9500#
NOC-NX9500#terminal length 30
NOC-NX9500#terminal width 100
NOC-NX9500#show terminal
Terminal Type: xterm
Length: 30 Width: 100
NOC-NX9500#
```

### Related Commands

```
no (user exec mode) on Resets the width or length of the terminal window
page 83
no (priv-exec-mode) on Resets the width or length of the terminal window
page 189
```

### *time-it (user and privi exec modes)*

Verifies the time taken by a particular command between request and response



#### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
time-it <COMMAND>
```

### Parameters

```
time-it <COMMAND>
```

```
time-it <COMMAND> Verifies the time taken by a particular command to execute and provide a result
```

- <COMMAND> – Specify the command.

### Examples

```
ap8432-070235>time-it enable
That took 0.00 seconds..
ap8432-070235#
```

### Example (Privi Exec Mode)

```
rfs4000-229D58#time-it config terminal
Enter configuration commands, one per line. End with CNTL/Z.
That took 0.00 seconds..
rfs4000-229D58(config)#
```



---

### *traceroute* (user-privi-exec-mode)

Traces the route to a defined destination

Use '--help' or '-h' to display a complete list of parameters for the traceroute command

---



#### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

---

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
traceroute <LINE>
```

#### Parameters

```
traceroute <LINE>
```

|                   |                                                              |
|-------------------|--------------------------------------------------------------|
| traceroute <LINE> | Traces the route to a destination IP address or hostname     |
|                   | • <LINE> - Specify the destination IPv4 address or hostname. |

#### Example (User Exec Mode)

```
NOC-NX9500>traceroute 10.234.160.13
traceroute to 10.234.160.13 (10.234.160.13), 30 hops max, 46 byte packets
 1 10.234.160.13 (10.234.160.13) 0.315 ms 0.159 ms 0.137 ms
NOC-NX9500>
```

#### Example (Privi Exec Mode)

```
NOC-NX9500#traceroute 10.234.160.11
traceroute to 10.234.160.11 (10.234.160.11), 30 hops max, 46 byte packets
 1 10.234.160.11 (10.234.160.11) 8.115 ms 0.410 ms 0.370 ms
NOC-NX9500#
```

### *traceroute6* (user-privi-exec-mode)

Traces the route to a specified IPv6 destination

---



#### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

---

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
traceroute6 <LINE>
```

## Parameters

```
traceroute6 <LINE>
```

|                    |                                                                                                                                                                               |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| traceroute6 <LINE> | Traces the route to a destination IPv6 address or hostname <ul style="list-style-type: none"><li>• &lt;LINE&gt; - Specify the destination IPv6 address or hostname.</li></ul> |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Example (User Exec Mode)

```
rfs4000-6DB5D4>traceroute6 2001:10:10:10:10:10:10:1
traceroute to 2001:10:10:10:10:10:10:1 (2001:10:10:10:10:10:10:1) from
2001:10:10:10:10:10:10:2, 30 hops max, 16 byte packets
 1 2001:10:10:10:10:10:10:1 (2001:10:10:10:10:10:10:1) 6.054 ms 0.448 ms 0.555 ms
rfs4000-6DB5D4>
```

## Example (Privileged Exec Mode)

```
rfs4000-229D587#traceroute6 2001:10:10:10:10:10:10:2
traceroute to 2001:10:10:10:10:10:10:2 (2001:10:10:10:10:10:10:2) from
2001:10:10:10:10:10:10:1, 30 hops max, 16 byte packets
 1 2001:10:10:10:10:10:10:2 (2001:10:10:10:10:10:10:2) 0.622 ms 0.497 ms 0.531 ms
rfs4000-229D587#
```

## upgrade

Upgrades a device's software image

## Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000, RFS 6000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
upgrade [<FILE>|<URL>|dhcp-vendor-options]
upgrade [<FILE>|<URL>] {background|on <DEVICE-NAME>|on <RF-DOMAIN-NAME>}
upgrade dhcp-vendor-options {<DEVICE-NAME>|on <RF-DOMAIN-NAME>}
upgrade dhcp-vendor-options {<DEVICE-NAME>} {<DEVICE-NAME>}
upgrade dhcp-vendor-options {on <RF-DOMAIN-NAME>} {containing <SUB-STRING>|exclude-
controllers|
exclude-rf-domain-managers|filter <DEVICE-TYPE>}
```

## Parameters

```
upgrade [<FILE>|<URL>] {background|on <DEVICE-NAME>|on <RF-DOMAIN-NAME>}
```

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <FILE>              | Specify the target firmware image location in the following format:<br>cf:/path/file<br>usb1:/path/file<br>usb2:/path/file<br>usb<n>:/path/file                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <URL>               | Specify the target firmware image location. Use one of the following formats: <ul style="list-style-type: none"> <li>IPv4 URLs: <ul style="list-style-type: none"> <li>tftp://&lt;hostname IP&gt;[:port]/path/file</li> <li>ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IP&gt;[:port]/path/file</li> <li>sftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IP&gt;[:port]/path/file</li> <li>http://&lt;hostname IP&gt;[:port]/path/file</li> <li>cf:/path/file</li> <li>usb&lt;n&gt;:/path/file</li> </ul> </li> <li>IPv6 URLs: <ul style="list-style-type: none"> <li>tftp://&lt;hostname IPv6&gt;[:port]/path/file</li> <li>ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IPv6&gt;[:port]/path/file</li> <li>sftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IPv6&gt;[:port]/path/file</li> <li>http://&lt;hostname IPv6&gt;[:port]/path/file</li> </ul> </li> </ul> |
| background          | Optional. Performs upgrade in the background                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| on <DEVICE-NAME>    | Optional. Upgrades the software image on a specified remote device <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| on <RF-DOMAIN-NAME> | Optional. Upgrades the software image on all devices within a specified RF Domain <ul style="list-style-type: none"> <li>&lt;RF-DOMAIN-NAME&gt; - Specify the name of the RF Domain.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

```
upgrade dhcp-vendor-options {<DEVICE-NAME>} {<DEVICE-NAME>}
```

|                                  |                                                                                                                                                                                                                                                                                                                      |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dhcp-vendor-options              | Uses DHCP vendor options to upgrade device(s)                                                                                                                                                                                                                                                                        |
| <DEVICE-NAME><br>{<DEVICE-NAME>} | Optional. Uses DHCP vendor options to upgrade a specified device. Specify the name of the AP, wireless controller, or service platform. <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; - Optional. You can optionally specify multiple comma-separated device names/MAC addresses to upgrade.</li> </ul> |

```
upgrade dhcp-vendor-options {on <RF-DOMAIN-NAME>} {containing <SUB-STRING>/
exclude-controllers/exclude-rf-domain-managers/filter <DEVICE-TYPE>}
```

|                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dhcpc-vendor-options                                                                                                              | Uses DHCP vendor options to upgrade device(s)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| on <RF-DOMAIN-NAME><br>{containing <SUB-STRING> <br>exclude-controllers  exclude-rf-<br>domain-managers  filter<br><DEVICE-TYPE>} | <p>Optional. Uses DHCP vendor options to upgrade all devices or specified device(s) within the RF Domain identified by the &lt;RF-DOMAIN-NAME&gt; keyword</p> <ul style="list-style-type: none"> <li>• &lt;RF-DOMAIN-NAME&gt; – Specify the RF Domain name. After specifying the RF Domain, optionally use the filters provided to identify specific device(s) within the RF Domain. If none of the filters are used, all devices within the RF Domain are upgraded. These filters are: <ul style="list-style-type: none"> <li>• containing &lt;SUB-STRING&gt; – Optional. Upgrades all devices, within the specified RF Domain, containing a specified sub-string in their hostname <ul style="list-style-type: none"> <li>&lt;SUB-STRING&gt; – Specify the sub-string to match.</li> </ul> </li> </ul> </li> <li>• exclude-controllers – Optional. Upgrades all devices, within the specified RF Domain, excluding controllers. Since only a NOC controller is capable of adopting other controllers, use this option when executing the command on a NOC controller.</li> <li>• exclude-rf-domain-manager – Optional. Upgrades all devices, within the specified RF Domain, excluding RF Domain managers. Use this option when executing the command on the NOC, Site controller, or RF Domain manager.</li> <li>• filter &lt;DEVICE-TYPE&gt; – Optional. Executes the command on all devices, within the specified RF Domain, of a specified type <ul style="list-style-type: none"> <li>• &lt;DEVICE-TYPE&gt; – Specify the device type. The options are:AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533, RFS 4000, RFS 6000, NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000. Upgrades all devices of the type specified here. For example, if AP 7602 is the device-type specified, all AP 7602 within the specified RF Domain are upgraded.</li> </ul> </li> </ul> |

**Example**

```

nx9500-6C8809#show boot

 IMAGE BUILD DATE INSTALL DATE VERSION

 Primary 02/05/2017 14:33:58 02/11/2017 12:27:53 5.9.1.0-024D
 Secondary 02/01/2017 21:36:24 02/03/2017 12:05:48 5.9.1.0-007D

Current Boot : Secondary
Next Boot : Primary
Software Fallback : Enabled
VM support : Not presentt
nx9500-6C8809#
nx9500-6C8809#upgrade ftp://anonymous:anonymous@192.168.13.10/LatestBuilds/W59/NX9500.img
Running from partition /dev/sda7
Validating image file header
Removing other partition
Making file system
Extracting files (this may take some
time).....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

```

```

.....
.....
.....
Control C disabled
Version of firmware update file is 5.9.2.0-026D
Removing unneeded files from flash:/crashinfo directory
Removing unneeded files from flash:/var2/log directory
Creating LILO files
Running LILO
Successful
nx9500-6C8809#
nx9500-6C8809#show boot

```

| IMAGE          | BUILD DATE                 | INSTALL DATE               | VERSION             |
|----------------|----------------------------|----------------------------|---------------------|
| <b>Primary</b> | <b>01/02/2018 12:03:13</b> | <b>01/10/2018 10:12:53</b> | <b>5.9.2.0-026D</b> |
| Secondary      | 02/01/2017 21:36:24        | 02/03/2017 12:05:48        | 5.9.1.0-007D        |

```

Current Boot : Secondary
Next Boot : Primary
Software Fallback : Enabled
VM support : Not present
nx9500-6C8809#

```



**Note**

After upgrading, the device has to be reloaded to boot using the new image.

The following example shows an RFS 6000 being upgraded via the controller:

```

nx7500-7F3609#upgrade tftp://192.168.0.50/RFS6000-5.9.2.0-026D.img rfs6000-6DCBB3

```

| DEVICE         | STATUS  | MESSAGE |
|----------------|---------|---------|
| rfs6000-6DCBB3 | Success | None    |

```

nx7500-7F3609#

```

The following example shows the upgrade status:

```

nx7500-7F3609#show upgrade detail
Last Image Upgrade Status : Successful
Last Image Upgrade Time : 2018-01-11 10:31:12

Running from partition /dev/sda7
var2 is 2 percent full
/tmp is 2 percent full
Free Memory 15258044 kB
FWU invoked via Linux shell
Validating image file header
Removing other partition
Making file system
Extracting files (this may take some time).
Control C disabled
Version of firmware update file is 5.9.2.0-026D
Creating LILO files
Running LILO
Successful

nx7500-7F3609#
nx7500-7F3609#show upgrade on rfs6000-6DCBB3
Last Image Upgrade Status :Successful
Last Image Upgrade Time :2018-01-11 10:31:12
nx7500-7F3609#

```

## Related Commands

`no (priv-exec-mode) on` Removes a patch installed on a specified device  
page 189

### *upgrade-abort*

Aborts an ongoing software image upgrade

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000, RFS 6000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
upgrade-abort {on <DEVICE-OR-DOMAIN-NAME>}
```

#### Parameters

```
upgrade-abort {on <DEVICE-OR-DOMAIN-NAME>}
```

|                            |                                                                                                                                                                                                                                                       |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| upgrade-abort              | Aborts an ongoing software image upgrade                                                                                                                                                                                                              |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Aborts an ongoing software image upgrade on a specified device or domain <ul style="list-style-type: none"><li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; - Specify the name of the AP, wireless controller, service platform, or RF Domain.</li></ul> |

#### Examples

```
rfs4000-229D58#upgrade ftp://anonymous:anonymous@192.168.13.10/LatestBuilds/W59/
RFS4000-5.9.2.0-026D.img
Running from partition /dev/mtdblock6
Validating image file header
Making file system
Extracting files (this may take some time).....
rfs4000-6DB5D4#upgrade-abort on rfs4000-229D58
rfs4000-229D58#upgrade ftp://anonymous:anonymous@192.168.13.10/LatestBuilds/W59/
RFS4000-5.9.2.0-026D.img
Running from partition /dev/mtdblock6
Validating image file header
Making file system
Extracting files (this may take some time).....
Update error: Aborted
rfs4000-229D588#
```

### *virtual-machine (user and privi exec modes)*

Installs, configures, and monitors the status of virtual machines (VMs)



#### Note

This command and its syntax is common to both the *User Executable* and *Privilege Executable* configuration modes.

## Supported in the following platforms:

- Service Platforms — NX 95XX, NX 96XX, VX 9000

## Syntax

```
virtual-machine [assign-usb-ports|console|export|install|restart|set|start|stop|uninstall]
virtual-machine assign-usb-ports team-vowlan {on <DEVICE-NAME>}
virtual-machine export <VM-NAME> [<FILE>|<URL>] {on <DEVICE-NAME>}
virtual-machine install [<VM-NAME>|adsp|team-urc|team-rls|team-vowlan]
virtual-machine restart [<VM-NAME>|hard|adsp|team-urc|team-rls|team-vowlan]
virtual-machine set [autostart|memory|vcpus|vif-count|vif-mac|vif-to-vmif|vnc]
virtual-machine set [autostart [ignore|start]|memory <512-8192>|vcpus <1-4>|
vif-count <0-2>|vif-mac <VIF-INDEX> <MAC-INDEX>|vif-to-vmif <VIF-INDEX> <VMIF-INDEX>|
vnc [disable|enable]] [<VM-NAME>|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}
```

The following virtual-machine commands are supported only on the VX 9000 platform:

```
virtual-machine volume-group [add-drive|replace-drive|resize-drive|resize-volume-group]
virtual-machine volume-group [add-drive|replace-drive] <BLOCK-DEVICE-LABEL>
virtual-machine volume-group replace-drive <BLOCK-DEVICE-LABLE> <NEW-BLOCK-DEVICE-
LABEL>
virtual-machine volume-group resize-volume-group <BLOCK-DEVICE-LABEL>
```

## Parameters

```
virtual-machine assign-usb-ports team-vowlan {on <DEVICE-NAME>}
```

|                              |                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| assign-usb-ports team-vowlan | Assigns USB ports to TEAM-VoWLAN on a specified device <ul style="list-style-type: none"><li>• on &lt;DEVICE-NAME&gt; - Optional. Specify the device name.</li></ul> <p><b>Note:</b> Use the <b>no &gt; virtual-machine &gt; assign-usb-ports</b> command to reassign the port to WiNG.</p> <p><b>Note:</b> TEAM-RLS VM cannot be installed when USB ports are assigned to TEAM-VoWLAN.</p> |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
virtual-machine export <VM-NAME> [<FILE>|<URL>] {on <DEVICE-NAME>}
```

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| virtual-machine export | <p>Exports an existing VM image and settings. Use this command to export the VM to another device in the same domain.</p> <ul style="list-style-type: none"> <li>• &lt;VM-NAME&gt; - Specify the VM name.</li> <li>• &lt;FILE&gt; - Specify the location and name of the source file (VM image). The VM image is retrieved and exported from the specified location.</li> <li>• &lt;URL&gt; - Specify the destination location. This is the location to which the VM image is copied. Use one of the following formats to provide the destination path: <ul style="list-style-type: none"> <li>tftp://&lt;hostname IP&gt;[:port]/path/file</li> <li>ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IP&gt;[:port]/path/file</li> <li>sftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IP&gt;[:port]/path/file</li> <li>http://&lt;hostname IP&gt;[:port]/path/file</li> </ul> </li> <li>• on &lt;DEVICE-NAME&gt; - Optional. Executes the command on a specified device or devices <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; - Specify the service platform name. In case of multiple devices, list the device names separated by commas.</li> </ul> </li> </ul> <p><b>Note:</b> The VM should be in a stop state during the export process.</p> <p><b>Note:</b> If the destination is a device, the image is copied to a predefined location (VM archive).</p> |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
virtual-machine install [<VM-NAME>|adsp|team-centro|team-rls|team-vowlan]
{on <DEVICE-NAME>}
```

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| virtual-machine install | <p>Installs the VM. The install command internally creates a VM template, consisting of the specified parameters, and starts the installation process.</p> <ul style="list-style-type: none"> <li>• &lt;VM-NAME&gt; - Specify the VM name.</li> <li>• adsp - Installs ADSP</li> <li>• team-centro - Installs the VM TEAM-Centro image</li> <li>• team-rls - Installs the VM TEAM-RLS image</li> <li>• team-vowlan - Installs the VM TEAM-VoWLAN image</li> </ul> <p>Specify the device on which to install the VM.</p> <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; - Optional. Executes the command on a specified device or devices <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; - Specify the service platform name. In case of multiple devices, list the device names separated by commas.</li> </ul> </li> </ul> |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
virtual-machine set [autostart [ignore|start]|memory <512-8192>|vcpus <1-4>|
vif-count <0-2>|vif-mac <VIF-INDEX> <MAC-INDEX>|vif-to-vmif <VIF-INDEX> <VMIF-INDEX>|vnc
[disable|enable]]
[<VM-NAME>|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}
```



virtual-machine  
set

Configures the VM settings

- autostart – Specifies whether to autostart the VM on system reboot
  - ignore – Enables autostart on each system reboot
  - start – Disables autostart
- memory – Defines the VM memory size
  - <512-8192> – Specify the VM memory from 512 - 8192 MB. The default is 1024 MB.
- vcpus – Specifies the number of VCPUS for this VM
  - <1-4> – Specify the number of VCPUS from 1- 4.
- vif-count – Configures or resets the VM's VIFs
  - <0-2> – Specify the VIF number from 0 - 2.
- vif-mac – Configures the MAC address of the selected virtual network interface
  - <1-2> – Select the VIF
    - <1-8> – Specify the MAC index for the selected VIF
    - <MAC> – Specify the customized MAC address for the selected VIF in the AA-BB-CC-DD-EE-FF format.

Each VM has a maximum of two network interfaces (indexed 1 and 2, referred to as VIF). By default, each VIF is automatically assigned a MAC from the range allocated for that device. However, you can use the 'set' keyword to specify the MAC from within the allocated range. Each of these VIFs are mapped to a layer 2 port in the dataplane (referred to as VMIF). These VMIFs are standard I2 ports on the DP bridge, supporting all VLAN and ACL commands. The WiNG software supports up to a maximum of 8 VMIFs. By default, a VM's interface is always mapped to VMIF1. You can map a VIF to any of the 8 VMIFs. Use the vif-to-vmif command to map a VIF to a VMIF on the DP bridge.

- vif-to-vmif – Maps the virtual interface (1 or 2) to the selected VMIF interface. Specify the VMIF interface index from 1 - 8.

WiNG provides a dataplane bridge for external network connectivity for VMs. VM Interfaces define which IP address is associated with each VLAN ID the service platform is connected to and enables remote service platform administration. Each custom VM can have up to a maximum of two VM interfaces. Each VM interface can be mapped to one of the twelve ports for NX 95XX on the dataplane bridge. This mapping determines the destination for service platform routing.

By default, VM interfaces are internally connected to the dataplane bridge via VMIF1. VMIF1, by default, is an untagged port providing access to VLAN 1 to support the capability to connect the VM interfaces to any of the VMIF ports. This provides the flexibility to move a VM interface onto different VLANs as well as configure specific firewall and QoS rules.

- vnc – Disables/enables VNC port option for an existing VM. When enabled, provides remote access to VGA through the noVNC client.
  - disable – Disables VNC port
  - enable – Enables VNC port

After configuring the VM settings, identify the VM to apply the settings.

- <VM-NAME> – Applies these settings to the VM identified by the <VM-NAME> keyword. Specify the VM name.
- adsp – Applies these settings to the ADSP VM
- team-urc – Applies these settings to the VM TEAM-URC
- team-rls – Applies these settings to the VM TEAM-RLS
- team-vowlan – Applies these settings to the VM TEAM-VoWLAN

```
virtual-machine start [<VM-NAME>|adsp|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}
```

virtual-machine start

Starts the VM, based on the parameters passed. Select one of the following options:

- <VM-NAME> - Starts the VM identified by the <VM-NAME> keyword. Specify the VM name.
- adsp - Starts the ADSP VM
- team-urc - Starts the VM TEAM-URC
- team-rls - Starts the VM TEAM-RLS
- team-vowlan - Starts the VM TEAM-VoWLAN

The following keywords are common to all of the above parameters:

- on <DEVICE-NAME> - Optional. Executes the command on a specified device or devices
  - <DEVICE-NAME> - Specify the service platform name. In case of multiple devices, list the device names separated by commas.

```
virtual-machine stop [<VM-NAME>|adsp|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}
```

virtual-machine stop hard

Stops the VM, based on the parameters passed. Select one of the following options:

- <VM-NAME> - Stops the VM identified by the <VM-NAME> keyword. Specify the VM name.
- ADSP - Stops the ADSP VM
- team-urc - Stops the VM TEAM-URC
- team-rls - Stops the VM TEAM-RLS
- team-vowlan - Stops the VM TEAM-VoWLAN

The following keywords are common to all of the above parameters:

- on <DEVICE-NAME> - Optional. Executes the command on a specified device or devices
  - <DEVICE-NAME> - Specify the service platform name. In case of multiple devices, list the device names separated by commas. Note: The option 'hard' forces the selected VM to shutdown.

**Note:** The option 'hard' forces the selected VM to shutdown.

```
virtual-machine uninstall [<VM-NAME>|adsp|team-urc|team-rls|team-vowlan] {on <DEVICE-NAME>}
```

virtual-machine uninstall

Uninstalls the specified VM

- <VM-NAME> - Uninstalls the VM identified by the <VM-NAME> keyword. Specify the VM name.
- ADSP - Uninstalls the ADSP VM
- team-urc - Uninstalls the VM TEAM-URC
- team-rls - Uninstalls the VM TEAM-RLS
- team-vowlan - Stops the VM TEAM-VoWLAN

The following keywords are common to all of the above parameters:

- on <DEVICE-NAME> - Optional. Executes the command on a specified device or devices
  - <DEVICE-NAME> - Specify the service platform name. In case of multiple devices, list the device names separated by commas.

**Note:** This command releases the VM's resources, such as memory, VCPUS, VNC port, disk space, and removes the RF Domain reference from the system.

```
virtual-machine volume-group [add-drive|resize-drive] <BLOCK-DEVICE-LABEL>
```

|                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>virtual-machine volume-group [add-drive] [resize-drive] &lt;BLOCK- DEVICE- LABEL&gt;]</pre> | <p>Enables provisioning of logical volume-groups on the VX 9000 platform. Logical volume-groups are created on the primary storage device, allowing the database storage to be expanded to include additional storage drives. However, volume-groups can be provisioned only on new VX 9000 installation and cannot be added to existing VX 9000 installation.</p> <p><b>Note:</b> The logical volume-group is supported only on a VX 9000 running the WiNG 5.9.1 and above version.</p> <ul style="list-style-type: none"> <li>• <b>add-drive</b> – Adds a new block-device to the VM. Note, currently a maximum of 3 (three) block devices can be added. To add a new drive, first halt the VM, In the Hypervisor, add a new storage disk to the VM and restart the VM. Once the VM comes up, use this command to add the new drive. To identify the new drive execute the <b>show &gt; virtual-machine &gt; volume-group &gt; status</b> command.</li> <li>• <b>resize-drive</b> - Resizes a drive in the VM's volume group. To increase the size of a drive in the volume-group, first halt the VM. In the Hypervisor, increase the size of the existing secondary storage drive and restart the VM. Once the VM comes up, use this command to resize the drive. To identify the drive with the additional free space, execute the <b>show &gt; virtual-machine &gt; volume-group &gt; status</b> command.</li> </ul> <p>The following keyword is common to all of the above parameters:</p> <ul style="list-style-type: none"> <li>• <b>&lt;BLOCK-DEVICE-LABEL&gt;</b> -Specify the block-device label to be added or resized depending on the action being performed.</li> </ul> |
|--------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
virtual-machine volume-group replace-drive <BLOCK-DEVICE-LABEL> <NEW-BLOCK-DEVICE-LABEL>
```

|                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>virtual-machine volume-group replace-drive &lt;BLOCK- DEVICE-LABEL&gt; &lt;NEW- BLOCK-DEVICE-LABEL&gt;]</pre> | <p>Enables provisioning of VMs as logical volume-groups on the VX 9000 platform. Logical volume-group VMs are created on the primary storage device, allowing the database storage to be expanded to include additional storage drives.</p> <ul style="list-style-type: none"> <li>• <b>replace-drive</b> – Replaces an existing block-device with a new block-device in a volume-group. To replace a drive in the volume-group, first halt the VM. In the Hypervisor, add the new drive and restart the VM. Once the VM comes up, use this command to replace an existing drive with the new drive. To identify the drive with the additional free space, execute the <b>show &gt; virtual-machine &gt; volume-group &gt; status</b> command <ul style="list-style-type: none"> <li>• <b>&lt;BLOCK-DEVICE-LABEL&gt;</b> -Specify the block-device label to be replaced.</li> <li>• <b>&lt;BLOCK-DEVICE-LABEL&gt;</b> - Specify the replacement block-device label.</li> </ul> </li> </ul> |
|--------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
virtual-machine volume-group resize-volume-group <BLOCK-DEVICE-LABEL>
```

|                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>virtual-machine volume- group resize-volume-group &lt;BLOCK-DEVICE-LABEL&gt;</pre> | <p>Enables provisioning of VMs as logical volume-groups on the VX 9000 platform. Logical volume-group VMs are created on the primary storage device, allowing the database storage to be expanded to include additional storage drives</p> <ul style="list-style-type: none"> <li>• <b>resize-volume-group</b> – Adds drive space to an existing block-device in the volume-group <ul style="list-style-type: none"> <li>• <b>&lt;BLOCK-DEVICE-LABEL&gt;</b> -Specify the block-device label to which additional drive space is to be provided</li> </ul> </li> </ul> |
|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

The following examples show the VM installation process:

### Insatllation media: USB

```
<DEVICE>#virtual-machine install <VM-NAME> type iso disk-size 8 install-media usb1://vms/
win7.iso autostart start memory 512 vcpus 3 vif-count 2 vnc enable
```

## Installation media: pre-installed disk image

```
<DEVICE>#virtual-machine install <VM-NAME> type disk install-media flash:/vms/
win7_disk.img autostart start memory 512 vcpus 3 vif-count 2 vnc-enable on <DEVICE-NAME>
In the preceding example, the command is executed on the device identified by the <DEVICE-
NAME> keyword. In such a scenario, the disk-size is ignored if specified. The VM has the
install media as first boot device.
```

## Installation media: VM archive

```
<DEVICE>#virtual-machine install type vm-archive install-media flash:/vms/<VM-NAME> vcpus 3
In the preceding example, the default configuration attached with the VM archive overrides
any parameters specified.
```

## Exporting an installed VM:

```
<DEVICE>#virtual-machine export <VM-NAME> <URL> on <DEVICE-NAME>
In the preceding example, the command copies the VM archive on to the URL (VM should be in
stop state).
<DEVICE>>virtual-machine install team-urc
Virtual Machine install team-urc command successfully sent.
<DEVICE>>
VX 9000-DE6F97>virtual-machine add-drive sdb
VX 9000-DE6F97>show virtual-machine volume-group status

Logical Volume: lv1

STATUS : available
SIZE : 81.89 GiB
VOLUME GROUP : vg0
PHYSICAL VOLUMES :
 sda10 : 73.90 GiB
 sdc1 : 8.00 GiB
AVAILABLE DISKS :
 sdb : size: 8590MB

* indicates a drive that must be resized

VX 9000-DE6F97>
```

## *exit (privi exec mode)*

Ends the current CLI session and closes the session window

For more information, see [exit](#).

## Supported in the following platforms:

- Access Points — AP 6522, AP 6532, AP 6562, AP 7502, AP 7522, AP 7532, AP 7161, AP 81XX, AP 8232
- Wireless Controllers — RFS 4000, RFS 6000
- Service Platforms — NX 7500, NX 9500, NX 9510

## Syntax

```
exit
```

## Parameters

None

## Examples

```
<exsw1>#exit
```

---

## raid

Enables *Redundant Array of Independent Disks* (RAID) management

RAID is a group of one or more independent, physical drives, referred to as an array or drive group. These physically independent drives are linked together and appear as a single storage unit or multiple virtual drives. Replacing a single, large drive system with an array, improves performance (input and output processes are faster) and increases fault tolerance within the data storage system.

In an array, the drives can be organized in different ways, resulting in different RAID types. Each RAID type is identified by a number, which determines the RAID level. The common RAID levels are 0, 00, 1, 5, 6, 50 and 60. The WiNG MegaRAID implementation supports RAID-1, which provides data mirroring, but does not support data parity. RAID-1 consists of a two-drive array, where the data is simultaneously written on both drives, ensuring total data redundancy. In case of a drive failure the information on the other drive is used to rebuild the failed drive.

An array is said to be degraded when one of its drives has failed. A degraded array continues to function and can be rebooted using the one remaining functional drive. When a drive fails, the chassis sounds an alarm (if enabled), and the CLI prompt changes to “RAID degraded”. The failed drive is automatically replaced with a hot spare (provided a spare is installed). The spare is used to re-build the array.

Use this command to:

- Verify the current array status
- Start and monitor array consistency checks
- Retrieve date and time of the last consistency check
- Shut down drives before physically removing them
- Install new drives
- Assign drives as hot spares
- Identify a degraded drive
- Deactivate an alarm (triggered when a drive is removed from the array)

### Supported in the following platforms:

- Service Platforms — NX 9500, NX 7500

---

#### Note



The NX 9500 service platform includes a single Intel MegaRAID controller, configured to provide a single virtual drive. This virtual drive is of the RAID-1 type, and has a maximum of two physical drives. In addition to these two drives, there are three hot spares, which are used in case of a primary drive failure.

---

#### Syntax

```
raid [check|install|locate|remove|silence|spare]
raid [check|silence]
raid [install|locate|remove|spare] drive <0-4>
```

#### Parameters

```
raid [check|silence]
```

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| check   | Starts a consistency check on the RAID array. Use the show > raid command to view consistency check status.<br>A consistency check verifies the data stored in the array. When regularly executed, it helps protect against data corruption, and ensures data redundancy. Consistency checks also warn of potential disk failures.                                                                                                            |
| silence | Deactivates an alarm<br><b>Note:</b> When enabled, an audible alarm is triggered when a drive in the array fails. The silence command deactivates the alarm (sound).<br><b>Note:</b> To enable RAID alarm, in the device configuration mode, use the raid > alarm > enable command. A NX 9500 profile can also have the RAID alarm feature activated. For more information on the enabling RAID alarm, see <a href="#">raid</a> on page 1284. |

**raid** [install|locate|remove|spare] drive <0-4>

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| install <0-4> | Includes a new drive, inserted in one of the available slots, in the array. Specify the drive number.<br><b>Note:</b> Drives 0 and 1 are the array drives. Drives 2, 3, and 4 are the hot spare drives. You can include the new drive in a degraded array, or enable it as a hot spare.<br><b>Note:</b> If the array is in a degraded state, the re-build process is triggered and the new drive is used to repair the degraded array. |
| locate <0-4>  | Enables LEDs to blink on a specified drive. Specify the drive number.<br><b>Note:</b> Blinking LEDs enable you correctly locate a drive.                                                                                                                                                                                                                                                                                               |
| remove <0-4>  | Removes (shuts down) a disk from the array, before it is physically removed from its slot. Specify the drive number containing the disk.<br><b>Note:</b> Use this command to also remove a hot spare.                                                                                                                                                                                                                                  |
| spare <0-4>   | Converts an unused drive into a hot spare. Specify the drive number.                                                                                                                                                                                                                                                                                                                                                                   |

### Example

```
nx9500-6C874D#raid install drive 0
Error: Input Error: Drive 0 is already member of array, can't be added
nx9500-6C874D#
nx9500-6C8809#raid spare drive 1
Error: RAID operation failed, returned 2, output: Input Error: Drive 1 is member of array,
can't be a hotspare
/
nx9500-6C8809#
```

### watch

Repeats a specified CLI command at periodic intervals

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6532, AP 6562, AP 7502, AP 7522, AP 7532, AP 7161, AP 81XX, AP 8232
- Wireless Controllers — RFS 4000, RFS 6000
- Service Platforms — NX 7500, NX 9500, NX 9510

#### Syntax

```
watch <1-3600> <LINE>
```

#### Parameters

```
watch <1-3600> <LINE>
```

---

|                |                                                                                         |
|----------------|-----------------------------------------------------------------------------------------|
| watch <1-3600> | Repeats a CLI command at a specified interval                                           |
| <1-3600>       | Select an interval from 1- 3600 seconds. Pressing CTRL-Z halts execution of the command |
| <LINE>         | Specify the CLI command name.                                                           |

**Examples**

```
<exsw1>#watch 1 show clock
<exsw1>#
```

# GLOBAL CONFIG MODE COMMANDS

## GLOBAL CONFIGURATION COMMANDS

---

This chapter summarizes the global-configuration commands in the CLI command structure.

The term global indicates characteristics or features effecting the system as a whole. Use the Global Configuration Mode to configure the system globally, or enter specific configuration modes to configure specific elements (such as interfaces or protocols). Use the configure terminal command (under PRIV EXEC) to enter the global configuration mode.

The following example describes the process of entering the global configuration mode from the privileged EXEC mode:

```
<DEVICE>#configure terminal
<DEVICE> (config)#
```



### Note

The system prompt changes to indicate you are now in the global configuration mode. The prompt consists of the device host name followed by (config) and a pound sign (#).

---

Commands entered in the global configuration mode update the running configuration file as soon as they are entered. However, these changes are not saved in the startup configuration file until a **commit write memory** command is issued.

```
<DEVICE>(config)#?
Global configuration commands:
 aaa-policy Configure a
 authentication/accounting/authorization
 policy
 aaa-tacacs-policy Configure an
 authentication/accounting/authorization
 TACACS policy
 alias Alias
 ap621 AP621 access point
 ap622 AP622 access point
 ap650 AP650 access point
 ap6511 AP6511 access point
 ap6521 AP6521 access point
 ap6522 AP6522 access point
 ap6532 AP6532 access point
 ap6562 AP6562 access point
 ap71xx AP71XX access point
 ap7502 AP7502 access point
 ap7522 AP7522 access point
 ap7532 AP7532 access point
 ap7562 AP7562 access point
 ap7602 AP7602 access point
 ap7612 AP7612 access point
 ap7622 AP7622 access point
 ap7632 AP7632 access point
 ap7662 AP7662 access point
 ap81xx AP81XX access point
 ap82xx AP82XX access point
 ap8432 AP8432 access point
 ap8533 AP8533 access point
```



|                                    |                                                                                            |
|------------------------------------|--------------------------------------------------------------------------------------------|
| application                        | Configure an application                                                                   |
| application-group                  | Configure an application-group                                                             |
| application-policy                 | Configure an application policy                                                            |
| association-acl-policy             | Configure an association acl policy                                                        |
| auto-provisioning-policy           | Configure an auto-provisioning policy                                                      |
| bgp                                | BGP Configuration                                                                          |
| bonjour-gw-discovery-policy        | Bonjour Gateway discovery policy                                                           |
| bonjour-gw-forwarding-policy       | Bonjour Gateway forwarding policy                                                          |
| bonjour-gw-query-forwarding-policy | Bonjour Gateway Query forwarding policy                                                    |
| captive-portal                     | Configure a captive portal                                                                 |
| clear                              | Clear                                                                                      |
| client-identity                    | Client identity (DHCP Device Fingerprinting)                                               |
| client-identity-group              | Client identity group (DHCP Fingerprint Database)                                          |
| clone                              | Clone configuration object                                                                 |
| crypto-cmp-policy                  | CMP policy                                                                                 |
| customize                          | Customize the output of summary cli commands                                               |
| database-client-policy             | Configure database client policy                                                           |
| database-policy                    | Configure database policy                                                                  |
| device                             | Configuration on multiple devices                                                          |
| device-categorization              | Configure a device categorization object                                                   |
| dhcp-server-policy                 | DHCP server policy                                                                         |
| dhcpv6-server-policy               | DHCPv6 server related configuration                                                        |
| dns-whitelist                      | Configure a whitelist                                                                      |
| event-system-policy                | Configure a event system policy                                                            |
| ex3500                             | Ex3500 device                                                                              |
| ex3500-management-policy           | Configure a ex3500 management policy                                                       |
| ex3500-qos-class-map-policy        | Configure a ex3500 qos class-map policy                                                    |
| ex3500-qos-policy-map              | Configure a ex3500 qos policy-map                                                          |
| ex3524                             | EX3524 wireless controller                                                                 |
| ex3548                             | EX3548 wireless controller                                                                 |
| firewall-policy                    | Configure firewall policy                                                                  |
| global-association-list            | Configure a global association list                                                        |
| guest-management                   | Configure a guest management policy                                                        |
| help                               | Description of the interactive help system                                                 |
| host                               | Enter the configuration context of a device by specifying its hostname                     |
| igmp-snoop-policy                  | Create igmp snoop policy                                                                   |
| inline-password-encryption         | Store encryption key in the startup configuration file                                     |
| ip                                 | Internet Protocol (IP)                                                                     |
| ipv6                               | Internet Protocol version 6 (IPv6)                                                         |
| ipv6-router-advertisement-policy   | IPv6 Router Advertisement related configuration                                            |
| l2tpv3                             | L2tpv3 tunnel protocol                                                                     |
| mac                                | MAC configuration                                                                          |
| management-policy                  | Configure a management policy                                                              |
| meshpoint                          | Create a new MESHPOINT or enter MESHPOINT configuration context for one or more MESHPOINTS |
| meshpoint-qos-policy               | Configure a meshpoint quality-of-service policy                                            |
| mint-policy                        | Configure the global mint policy                                                           |
| nac-list                           | Configure a network access control list                                                    |
| no                                 | Negate a command or set its defaults                                                       |
| nsight-policy                      | Configure a Nsight policy                                                                  |
| nx45xx                             | NX45XX integrated services platform                                                        |
| nx5500                             | NX5500 wireless controller                                                                 |
| nx65xx                             | NX65XX integrated services platform                                                        |
| nx75xx                             | NX75XX wireless controller                                                                 |
| nx9000                             | NX9000 wireless controller                                                                 |

|                         |                                                                                  |
|-------------------------|----------------------------------------------------------------------------------|
| passpoint-policy        | Configure a passpoint policy                                                     |
| password-encryption     | Encrypt passwords in configuration                                               |
| profile                 | Profile related commands - if no parameters are given, all profiles are selected |
| radio-qos-policy        | Configure a radio quality-of-service policy                                      |
| radius-group            | Configure radius user group parameters                                           |
| radius-server-policy    | Create device onboard radius policy                                              |
| radius-user-pool-policy | Configure Radius User Pool                                                       |
| rename                  | Clone configuration object                                                       |
| replace                 | Replace configuration object                                                     |
| rf-domain               | Create a RF Domain or enter rf-domain context for one or more rf-domains         |
| rfs4000                 | RFS4000 wireless controller                                                      |
| rfs6000                 | RFS6000 wireless controller                                                      |
| rfs7000                 | RFS7000 wireless controller                                                      |
| roaming-assist-policy   | Configure a roaming-assist policy                                                |
| role-policy             | Role based firewall policy                                                       |
| route-map               | Dynamic routing route map Configuration                                          |
| routing-policy          | Policy Based Routing Configuration                                               |
| rtl-server-policy       | Configure a rtl server policy                                                    |
| schedule-policy         | Configure a schedule policy                                                      |
| self                    | Config context of the device currently logged into                               |
| sensor-policy           | Configure a sensor policy                                                        |
| smart-rf-policy         | Configure a Smart-RF policy                                                      |
| t5                      | T5 DSL switch                                                                    |
| url-filter              | Configure a url filter                                                           |
| url-list                | Configure a URL list                                                             |
| vx9000                  | VX9000 wireless controller                                                       |
| web-filter-policy       | Configure a web filter policy                                                    |
| wips-policy             | Configure a wips policy                                                          |
| wlan                    | Create a new WLAN or enter WLAN configuration context for one or more WLANs      |
| wlan-qos-policy         | Configure a wlan quality-of-service policy                                       |
| write                   | Write running configuration to memory or terminal                                |
| clrscr                  | Clears the display screen                                                        |
| commit                  | Commit all changes made in this session                                          |
| do                      | Run commands from Exec mode                                                      |
| end                     | End current mode and change to EXEC mode                                         |
| exit                    | End current mode and down to previous mode                                       |
| revert                  | Revert changes                                                                   |
| service                 | Service Commands                                                                 |
| show                    | Show running system information                                                  |

<DEVICE>(config)#

## global-config-commands

The following table summarizes the Global Configuration Mode commands:

**Table 6: Global Config Commands**

| Command                                              | Description                                                                                                                                                                                                                                  |
|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">aaa-policy</a> on page 235               | Creates a AAA policy and enters its configuration mode. This policy enables administrators to define access control within the network.                                                                                                      |
| <a href="#">aaa-tacacs-policy</a> on page 236        | Creates a AAA-TACACS policy and enters its configuration mode. This policy provides access control to network devices such as routers, network access servers, and other computing devices through centralized servers.                      |
| <a href="#">alias</a> on page 237                    | Configures network, VLAN, and service aliases                                                                                                                                                                                                |
| <a href="#">ap6522</a> on page 248                   | Adds an AP 6522 to the network                                                                                                                                                                                                               |
| <a href="#">ap6562</a> on page 248                   | Adds an AP 6562 to the network                                                                                                                                                                                                               |
| <a href="#">ap7161</a> on page 249                   | Adds an AP 7161 to the network                                                                                                                                                                                                               |
| <a href="#">ap7502</a> on page 250                   | Adds an AP 7502 to the network                                                                                                                                                                                                               |
| <a href="#">ap7522</a> on page 251                   | Adds an AP 7522 to the network                                                                                                                                                                                                               |
| <a href="#">ap7532</a> on page 251                   | Adds an AP 7532 to the network                                                                                                                                                                                                               |
| <a href="#">ap7562</a> on page 252                   | Adds an AP 7562 to the network                                                                                                                                                                                                               |
| <a href="#">ap7602</a> on page 253                   | Adds an AP 7602 to the network                                                                                                                                                                                                               |
| <a href="#">ap7612</a> on page 254                   | Adds an AP 7612 to the network                                                                                                                                                                                                               |
| <a href="#">ap7622</a> on page 254                   | Adds an AP 7622 to the network                                                                                                                                                                                                               |
| <a href="#">ap7632</a> on page 255                   | Adds an AP 7632 to the network                                                                                                                                                                                                               |
| <a href="#">ap7662</a> on page 256                   | Adds an AP 7662 to the network                                                                                                                                                                                                               |
| <a href="#">ap8163</a> on page 256                   | Adds an AP 8163 to the network                                                                                                                                                                                                               |
| <a href="#">ap8432</a> on page 257                   | Adds an AP 8432 to the network                                                                                                                                                                                                               |
| <a href="#">ap8533</a> on page 258                   | Adds an AP 8533 to the network                                                                                                                                                                                                               |
| <a href="#">application</a> on page 258              | Creates an application definition and enters its configuration mode. This command allows you to create a customized application detection definition.                                                                                        |
| <a href="#">application-policy</a> on page 267       | Creates an application group and enters its configuration mode                                                                                                                                                                               |
| <a href="#">application-group</a> on page 263        | Creates an application policy and enters its configuration mode. This policy defines the actions executed on recognized HTTP (e.g. Facebook), enterprise (e.g. Webex) and peer-to-peer (e.g. gaming) applications or application-categories. |
| <a href="#">association-acl-policy</a> on page 283   | Creates an association ACL policy and enters its configuration mode. This policy restricts access by specifying a client MAC address or range of addresses to either include or exclude from WLAN connectivity.                              |
| <a href="#">auto-provisioning-policy</a> on page 284 | Creates an auto provisioning policy and enters its configuration mode. This policy defines the process by which an access point discovers controllers and associates with it.                                                                |
| <a href="#">bgp</a> on page 285                      | Configures BGP (Border Gateway Protocol) settings                                                                                                                                                                                            |

**Table 6: Global Config Commands (continued)**

| Command                                                          | Description                                                                                                                                                                                                                                                      |
|------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">bonjour-gw-discovery-policy</a> on page 287          | Creates a Bonjour GW Discovery policy and enters its configuration mode. This policy configures the VLANs on which Bonjour services are located.                                                                                                                 |
| <a href="#">bonjour-gw-forwarding-policy</a> on page 291         | Configures a Bonjour GW Forwarding policy and enters its configuration mode. This policy enables the discovery of services on VLANs not visible to the device running the Bonjour Gateway.                                                                       |
| <a href="#">bonjour-gw-query-forwarding-policy</a> on page 292   | Creates a Bonjour GW Query Forwarding policy and enters its configuration mode. This policy enables Bonjour query forwarding across multiple VLANs.                                                                                                              |
| <a href="#">captive-portal</a> on page 293                       | Creates a captive portal and enters its configuration mode                                                                                                                                                                                                       |
| <a href="#">clear</a> on page 335                                | Clears the event history                                                                                                                                                                                                                                         |
| <a href="#">client-identity</a> on page 336                      | Creates a client identity definition and enters its configuration mode. This feature enables client identification through DHCP device fingerprinting.                                                                                                           |
| <a href="#">client-identity-group</a> on page 343                | Creates a new client identity group and enters its configuration mode                                                                                                                                                                                            |
| <a href="#">clone</a> on page 347                                | Clones a specified configuration object                                                                                                                                                                                                                          |
| <a href="#">crypto-cmp-policy</a> on page 348                    | Creates a crypto CMP (Certificate Management Protocol) policy and enters its configuration mode. CMP is an Internet protocol designed to obtain and manage digital certificates in a PKI (Public Key Infrastructure) network.                                    |
| <a href="#">customize</a> on page 349                            | Customizes the CLI command summary output                                                                                                                                                                                                                        |
| <a href="#">database-client-policy global-config</a> on page 359 | Creates a database client policy and enters its configuration mode. The database client policy configures the IP address or hostname of the VX 9000 hosting the captive-portal/NSight database. Use this option when deploying a split NSight/EGuest deployment. |
| <a href="#">database-policy global config</a> on page 363        | Creates a database policy and enters its configuration mode. This policy enables the database, and also configures the database replica set.                                                                                                                     |
| <a href="#">device</a> on page 368                               | Specifies configuration on multiple devices                                                                                                                                                                                                                      |
| <a href="#">device-categorization</a> on page 369                | Creates a device categorization list and enters its configuration mode. The list categorizes devices as sanctioned or neighboring. Categorization of devices enables quick identification and blocking of unsanctioned devices in the network.                   |
| <a href="#">dhcp-server-policy</a> on page 372                   | Creates a DHCP server policy and enters its configuration mode. This policy allows hosts on an IP network to request and be assigned IP addresses and discover information about the network.                                                                    |
| <a href="#">dhcpv6-server-policy</a> on page 373                 | Creates a DHCPv6 server policy and enters its configuration mode. This policy configures hosts with IPv6 addresses, IP prefixes and other configuration attributes required on an IPv6 network.                                                                  |
| <a href="#">dns-whitelist</a> on page 374                        | Creates a DNS whitelist and enters its configuration mode. A DNS whitelist is used with a captive portal to provide access services to requesting wireless clients.                                                                                              |

**Table 6: Global Config Commands (continued)**

| Command                                                      | Description                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">event-system-policy</a> on page 377              | Creates an Event system policy and enters its configuration mode. This policy enables administrators to create notification mechanisms using one, some, or all of the SNMP, syslog, controller forwarding, or email notification options available to the controller or service platform.   |
| <a href="#">ex3500</a> on page 391                           | Creates an EX3500 time range list and enters its configuration mode                                                                                                                                                                                                                         |
| <a href="#">ex3500-management-policy</a> on page 395         | Creates an EX3500 management policy and enters its configuration mode. This policy controls access to the EX3500 switch from management stations using SNMP.                                                                                                                                |
| <a href="#">ex3500-qos-class-map-policy</a> on page 411      | Creates an EX3500 QoS class map policy and enters its configuration mode. The QoS policy map assigns priority to mission critical EX3500 switch data traffic, prevent EX3500 switch bandwidth congestion, and prevent packet drops.                                                         |
| <a href="#">ex3500-qos-policy-map</a> on page 415            | Creates an EX3500 QoS policy map and enters its configuration mode. This policy defines rules that filter traffic exchanged between the EX3500 switch and its connected devices.                                                                                                            |
| <a href="#">ex3524</a> on page 425                           | Adds a EX3524 switch to the network                                                                                                                                                                                                                                                         |
| <a href="#">ex3548</a> on page 426                           | Adds a EX35XX switch to the network                                                                                                                                                                                                                                                         |
| <a href="#">firewall-policy</a> on page 427                  | Creates a firewall policy and enters its configuration mode. This policy configures safe guards against DoS (denial of service) attacks and packet storms. It also configures firewall parameters, such as logging, application layer gateway, TCP protocol checks, state flow checks, etc. |
| <a href="#">global-association-list</a> on page 428          | Configures a global list of client MAC addresses                                                                                                                                                                                                                                            |
| <a href="#">guest-management-policy</a> on page 431          | Creates a guest management policy and enters its configuration mode. This policy redirects guest users to a registration portal, upon association to a captive portal SSID (Service Set Identifier).                                                                                        |
| <a href="#">host</a> on page 440                             | Sets the system's network name                                                                                                                                                                                                                                                              |
| <a href="#">inline-password-encryption</a> on page 440       | Stores the encryption key in the startup configuration file                                                                                                                                                                                                                                 |
| <a href="#">iot-device-type-imagotag-policy</a> on page 441  | Creates an IoT Device-Type Imagotag policy and enters its configuration mode. This policy enables support for SES-imagotag's ESL tags on WiNG APs (with USB ports).                                                                                                                         |
| <a href="#">ip</a> on page 448                               | Creates a IP ACL (access control list) and/or a SNMP (Simple Network Management Protocol) ACL, and enters its configuration mode                                                                                                                                                            |
| <a href="#">ipv6</a> on page 450                             | Creates a IPv6 ACL and enters its configuration mode                                                                                                                                                                                                                                        |
| <a href="#">ipv6-router-advertisement-policy</a> on page 451 | Creates an IPv6 RA (router advertisement) policy and enters its configuration mode                                                                                                                                                                                                          |
| <a href="#">l2tpv3</a> on page 462                           | Configures L2TPv3 (Layer 2 Tunneling Protocol Version 3)tunnel policy and enters its configuration mode. This policy defines control and encapsulation protocols for tunneling layer 2 frames between two IP nodes.                                                                         |
| <a href="#">location-policy</a> on page 463                  | Configures a location policy and enters its configuration mode                                                                                                                                                                                                                              |

**Table 6: Global Config Commands (continued)**

| Command                                                        | Description                                                                                                                                                                                                 |
|----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">mac</a> on page 467                                | Configures MAC access lists (goes to the MAC (Access Control List) mode)                                                                                                                                    |
| <a href="#">management-policy</a> on page 468                  | Creates a management policy and enters its configuration context. This policy configures services that run on a device, such as welcome messages, banners, etc.                                             |
| <a href="#">meshpoint</a> on page 469                          | Creates a meshpoint and enters its configuration mode                                                                                                                                                       |
| <a href="#">meshpoint-qos-policy</a> on page 470               | Creates a meshpoint QoS (quality of service) policy and enters its configuration mode                                                                                                                       |
| <a href="#">mint-policy</a> on page 471                        | Creates a MiNT security policy and enters its configuration mode                                                                                                                                            |
| <a href="#">nac-list</a> on page 472                           | Creates a network ACL and enters its configuration mode                                                                                                                                                     |
| <a href="#">no (global-config-mode)</a> on page 475            | Negates a command or sets its default                                                                                                                                                                       |
| <a href="#">nsight-policy (global-config-mode)</a> on page 479 | Creates an NSight policy and enters its configuration mode                                                                                                                                                  |
| <a href="#">passpoint-policy</a> on page 486                   | Creates a new passpoint policy and enters its configuration mode                                                                                                                                            |
| <a href="#">password-encryption</a> on page 487                | Enables password encryption                                                                                                                                                                                 |
| <a href="#">profile</a> on page 488                            | Creates a device profile and enters its configuration mode                                                                                                                                                  |
| <a href="#">radio-qos-policy</a> on page 492                   | Creates a radio qos policy and enters its configuration mode                                                                                                                                                |
| <a href="#">radius-group</a> on page 493                       | Creates a RADIUS group and enters its configuration mode                                                                                                                                                    |
| <a href="#">radius-server-policy</a> on page 494               | Creates a RADIUS server policy and enters its configuration mode                                                                                                                                            |
| <a href="#">radius-user-pool-policy</a> on page 495            | Creates a RADIUS user pool policy and enters its configuration mode                                                                                                                                         |
| <a href="#">rename</a> on page 496                             | Renames an existing TLO (top-level object)                                                                                                                                                                  |
| <a href="#">replace</a> on page 497                            | Selects an existing device by its MAC address or hostname and replaces it with a new device having a different MAC address                                                                                  |
| <a href="#">rf-domain</a> on page 499                          | Creates an RF Domain and enters its configuration mode                                                                                                                                                      |
| <a href="#">rfs4000</a> on page 527                            | Adds an RFS 4000 to the network                                                                                                                                                                             |
| <a href="#">roaming-assist-policy</a> on page 530              | Configures a roaming assist policy and enters its configuration mode. This policy enables access points to assist wireless clients in making roaming decisions, such as which access point to connect, etc. |
| <a href="#">nx5500</a> on page 528                             | Adds an NX 5500 to the network                                                                                                                                                                              |
| <a href="#">nx75xx</a> on page 528                             | Adds an NX 7500 to the network                                                                                                                                                                              |
| <a href="#">nx9000</a> on page 529                             | Adds an NX 95XX or NX 96XX to the network                                                                                                                                                                   |
| <a href="#">role-policy</a> on page 531                        | Creates a role policy and enters its configuration mode                                                                                                                                                     |
| <a href="#">route-map</a> on page 532                          | Creates a dynamic BGP route map and enters its configuration mode                                                                                                                                           |
| <a href="#">routing-policy</a> on page 533                     | Creates a routing policy and enters its configuration mode                                                                                                                                                  |
| <a href="#">rtl-server-policy</a> on page 533                  | Creates an RTL server policy and enters its configuration mode. The RTL server policy provides the exact location (URL) at which the Euclid server can be reached.                                          |

**Table 6: Global Config Commands (continued)**

| Command                                       | Description                                                                                                                                  |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">schedule-policy</a> on page 536   | Creates a schedule policy and enters its configuration mode                                                                                  |
| <a href="#">self</a> on page 539              | Displays a logged device's configuration context                                                                                             |
| <a href="#">sensor-policy</a> on page 540     | Creates a sensor policy and enters its configuration mode                                                                                    |
| <a href="#">smart-rf-policy</a> on page 545   | Creates a Smart RF policy and enters its configuration mode                                                                                  |
| <a href="#">t5</a> on page 546                | Configures a t5 wireless controller. This command is applicable only on the RFS 4000, NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000 platforms. |
| <a href="#">web-filter-policy</a> on page 547 | Creates a Web Filtering policy and enters its configuration mode                                                                             |
| <a href="#">wips-policy</a> on page 553       | Creates a WIPS policy and enters its configuration mode                                                                                      |
| <a href="#">wlan</a> on page 554              | Creates a WLAN (Wireless Local Area Network) and enters its configuration mode                                                               |
| <a href="#">wlan-qos-policy</a> on page 622   | Creates a WLAN QoS policy and enters its configuration mode                                                                                  |
| <a href="#">url-filter</a> on page 623        | Creates an URL filter and enters its configuration mode. URL filtering is a licensed feature.                                                |
| <a href="#">url-list</a> on page 633          | Creates an URL list and enters its configuration mode.                                                                                       |
| <a href="#">vx9000</a> on page 636            | Configures a V-WLC (Virtual WLAN Controller) in a VM (virtual machine) environment                                                           |



**Note**

For more information on common commands (clrcsr, commit, help, revert, service, show, write, and exit), see [COMMON COMMANDS](#) on page 640.



**Note**

The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (\_) character.

*aaa-policy*

Configures an AAA (Authentication, Accounting, and Authorization) policy. Use an AAA policy to define access control within the network.

A controller, service platform, or access point can interoperate with external RADIUS and LDAP servers (AAA Servers) to provide an additional user database and authentication resource. Each WLAN can maintain its own unique AAA configuration. Up to six servers can be configured for providing AAA services.

**Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
aaa-policy <AAA-POLICY-NAME>
```

## Parameters

```
aaa-policy <AAA-POLICY-NAME>
```

|                   |                                                                           |
|-------------------|---------------------------------------------------------------------------|
| <AAA-POLICY-NAME> | Specify the AAA policy name. If the policy does not exist, it is created. |
|-------------------|---------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config)#aaa-policy test
nx9500-6C8809(config-aaa-policy-test)#?
AAA Policy Mode commands:
 accounting Configure accounting parameters
 attribute Configure RADIUS attributes in access and accounting
 requests
 authentication Configure authentication parameters
 health-check Configure server health-check parameters
 mac-address-format Configure the format in which the MAC address must be
 filled in the Radius-Request frames
 no Negate a command or set its defaults
 proxy-attribute Configure radius attribute behavior when proxying
 through controller or rf-domain-manager
 server-pooling-mode Configure the method of selecting a server from the
 pool of configured AAA servers
 use Set setting to use

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-aaa-policy-test)#
```

## Related Commands

|    |                                |
|----|--------------------------------|
| no | Removes an existing AAA policy |
|----|--------------------------------|



### Note

For more information on the AAA policy commands, see [AAA-POLICY](#).

## *aaa-tacacs-policy*

Configures AAA TACACS+ (Terminal Access Controller Access-Control System) policy. TACACS+ is a protocol created by CISCO Systems which provides access control to network devices such as routers, network access servers and other networked computing devices through one or more centralized servers. TACACS provides separate authentication, authorization, and accounting services running on different servers.

TACACS controls user access to devices and network resources while providing separate accounting, authentication, and authorization services. Some of the services provided by TACACS are:



- Authorizing each command with the TACACS+ server before execution.
- Accounting each session's logon and log off events.
- Authenticating each user with the TACACS+ server before enabling access to network resources.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
aaa-tacacs-policy <AAA-TACACS-POLICY-NAME>
```

#### Parameters

```
aaa-tacacs-policy <AAA-TACACS-POLICY-NAME>
```

<AAA-TACACS-POLICY-NAME> Specify the AAA-TACACS policy name. If the policy does not exist, it is created.

#### Examples

```
nx9500-6C8809(config)#aaa-tacacs-policy testpolicy
nx9500-6C8809(config-aaa-tacacs-policy-testpolicy)#?
AAA TACACS Policy Mode commands:
 accounting Configure accounting parameters
 authentication Configure authentication parameters
 authorization Configure authorization parameters
 no Negate a command or set its defaults

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-aaa-tacacs-policy-testpolicy)#
```

#### Related Commands

**no** Removes an existing AAA TACACS policy



#### Note

For more information on the AAA-TACACS policy commands, see [AAA-TACACS-POLICY](#).

#### alias

Configures the following types of aliases: network, VLAN, host, string, network-service, etc.

Aliases are objects having a unique name and content that is determined by the alias type (for example, network, VLAN, network-service, etc.).

---

A typical, large enterprise network, consists of multiple sites (RF Domains) having similar configuration parameters with few elements that vary, such as networks or network ranges, hosts having different IP addresses, and VLAN IDs or URLs. These elements can be defined as aliases (object oriented wireless firewalls) and used across sites by applying overrides to the object definition. Using aliases results in a configuration that is easier to understand and maintain.

Multiple instances of an alias (same type and same name) can be defined at any of the following levels: global, RF Domain, profile, or device. An alias defined globally functions as a TLO (top-level-object). Global aliases are not mandatory, and can be defined at the domain-level, or profile, or device-level only. An alias defined on a device is applicable to that device only. An alias defined on a profile applies to every device using the profile. Similarly, aliases defined at the RF Domain level apply to all devices within that domain.

Aliases defined at any given level can be overridden at any of the next lower levels. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence.

The different aliases types supported are:

- **address-range alias** – Maps a user-friendly name to a range of IP addresses. An address-range alias can be utilized at different deployments. For example, if an ACL defines a pool of network addresses as 192.168.10.10 through 192.168.10.100 for an entire network, and a remote location's network range is 172.16.13.20 through 172.16.13.110, the remote location's ACL can be overridden using an alias. At the remote location, the ACL works with the 172.16.13.20-110 address range. A new ACL need not be created specifically for the remote deployment location.
- **host alias** – Maps a user-friendly name to a specific host (identified by its IP address. For example, 192.168.10.23). A host alias can be utilized at different deployments. For example, if a central network DNS server is set a static IP address, and a remote location's local DNS server is defined, this host can be overridden at the remote location. At the remote location, the network is functional with a local DNS server, but uses the name set at the central network. A new host need not be created at the remote location. This simplifies creating and managing hosts and allows an administrator to better manage specific local requirements.
- **network alias** – Maps a user-friendly name to a network. A network alias can be utilized at different deployments. For example, if a central network ACL defines a network as 192.168.10.0/24, and a remote location's network range is 172.16.10.0/24, the ACL can be overridden at the remote location to suit their local (but remote) requirement. At the remote location, the ACL functions with the 172.16.10.0/24 network. A new ACL need not be created specifically for the remote deployment. This simplifies ACL definition and allows an administrator to better manage specific local requirements.
- **network-group alias** – Maps a user-friendly name to a single or a range of addresses of devices, hosts, and network configurations. Network configurations are complete networks in the form 192.168.10.0/24 or IP address range in the form 192.168.10.10-192.168.10.20.

A network-group alias can contain a maximum of eight (8) host entries, eight (8) network entries, and eight (8) IP address-range entries. A maximum of 32 network-group alias entries can be created.

A network-group alias can be used in IP firewall rules to substitute hosts, subnets, and IP address ranges.

- **network-service alias** – Maps a user-friendly name to service protocols and ports. Both source and destination ports are configurable. For each protocol, up to 2 source port ranges and up to 2 destination port ranges can be configured. A maximum of 4 protocol entries can be configured per

---

network-service alias. When used with an ACL, the network-service alias defines the service-specific components of the ACL rule. Overrides can be applied to the service alias, at the device level, without modifying the ACL. Application of overrides to the service alias allows an ACL to be used across sites.

Use a network-service alias to associate more than one IP address to a network interface, providing multiple connections to a network from a single IP node.

- **number alias** – Maps a user-friendly name to a number
- **vlan alias** – Maps a user-friendly name to a VLAN ID. A VLAN alias can be used at different deployments. For example, if a named VLAN is defined as 10 for the central network, and the VLAN is set at 26 at a remote location, the VLAN can be overridden at the deployment location with an alias. At the remote deployment location, the network is functional with a VLAN ID of 26, but utilizes the name defined at the centrally managed network. A new VLAN need not be created specifically for the remote deployment.
- **string alias** – Maps a user-friendly name to a specific string (for example, RF Domain name). A string alias can be utilized at different deployments. For example, if the main domain at a remote location is called *loc1.domain.com* and at another deployment location it is called *loc2.domain.com*, the alias can be overridden at the remote location to suit the local (but remote) requirement. At one remote location, the alias functions with the *loc1.domain.com* domain and at the other with the *loc2.domain.com* domain.
- **encrypted-string alias** – Maps a user-friendly name to a string value. The string value of this alias is encrypted when "password-encryption" is enabled. Encrypted-string aliases can be used for string configuration parameters that are encrypted by the "password-encryption" feature.
- **hashed-string alias** – Maps a user-friendly name to a hashed-string value. Hashed-string aliases can be used for string configuration parameters that are hashed, such as passwords.



#### Note

When used with ACLs, network, network-group, and network-service aliases act as enhanced firewalls.

---

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
alias [address-range|encrypted-string|hashed-string|host|network|network-group|
network-service|number|string|vlan]
alias address-range <ADDRESS-RANGE-ALIAS-NAME> <STARTING-IP> to <ENDING-IP>
alias encrypted-string <ENCRYPTED-STRING-ALIAS-NAME> [0|2] <LINE>
alias hashed-string <HASHED-STRING-ALIAS-NAME> <LINE>
alias host <HOST-ALIAS-NAME> <HOST-IP>
alias network <NETWORK-ALIAS-NAME> <NETWORK-ADDRESS/MASK>]
alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range|host|network]
alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range <STARTING-IP>
to <ENDING-IP> {<STARTING-IP> to <ENDING-IP>}|host <HOST-IP> {<HOST-IP>}|
network <NETWORK-ADDRESS/MASK> {<NETWORK-ADDRESS/MASK>}]
alias network-service <NETWORK-SERVICE-ALIAS-NAME> proto [<0-254>|<WORD>|eigrp|
gre|igmp|igmp|ospf|vrrp] {(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|
ldap|nntp|ntp|pop3|proto|sip|smtp|sourceport|ssh|telnet|tftp|www)}
alias number <NUMBER-ALIAS-NAME> <0-4294967295>
alias string <STRING-ALIAS-NAME> <LINE>
alias vlan <VLAN-ALIAS-NAME> <1-4094>
```

## Parameters

```
alias address-range <ADDRESS-RANGE-ALIAS-NAME> <STARTING-IP> to <ENDING-IP>
```

|                                          |                                                                                                                                                                                                                                                            |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| address-range <ADDRESS-RANGE-ALIAS-NAME> | Creates an address range alias, defining a range of IP addresses <ul style="list-style-type: none"><li>&lt;ADDRESS-RANGE-ALIAS-NAME&gt; - Specify the address range alias name.</li></ul> <p><b>Note:</b> Alias name should begin with '\$'.</p>           |
| <STARTING-IP> to <ENDING-IP>             | Associates a range of IP addresses with this address range alias <ul style="list-style-type: none"><li>&lt;STARTING-IP&gt; - Specify the first IP address in the range.</li><li>to &lt;ENDING-IP&gt; - Specify the last IP address in the range.</li></ul> |

```
alias encrypted-string <ENCRYPTED-STRING-ALIAS-NAME> [0|2] <LINE>
```

|                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>encrypted-string<br/>&lt;ENCRYPTED-STRING-ALIAS-NAME&gt;</p> | <p>Creates an alias for an encrypted string. Use this alias for string configuration values that are encrypted when "password-encryption" is enabled. For example, in the management-policy, use it to define the SNMP community string. For more information, see <a href="#">snmp-server</a> on page 1537 (management policy config mode).</p> <ul style="list-style-type: none"> <li>• &lt;ENCRYPTED-STRING-ALIAS-NAME&gt; - Specify the encrypted-string alias name.</li> </ul> <p><b>Note:</b> Alias name should begin with '\$'.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <p>[0]2] &lt;LINE&gt;</p>                                       | <p>Configures the value associated with the alias name specified in the previous step</p> <ul style="list-style-type: none"> <li>• [0]2] &lt;LINE&gt; - Configures the alias value</li> </ul> <p><b>Note:</b> If password-encryption is enabled, in the <b>show &gt; running-config</b> output, this clear text is displayed as an encrypted string, as shown below:</p> <pre> nx9500-6C8809(config)#show running-config !..... alias encrypted-string \$enString 2 fABMK2is7UToNiZE3MQXbgAAAxB0ZIysdqsEJwr6AH/Da// ! --More-- nx9500-6C8809 </pre> <p>In the above <b>show &gt; running-config</b> output, the '2' displayed before the encrypted-string alias value indicates that the displayed text is encrypted and not a clear text. However, if password-encryption is disabled the clear text is displayed as is:</p> <pre> nx9500-6C8809(config)#show running-config !..... ! alias encrypted-string \$enString 0 test11223344 ! --More-- nx9500-6C8809 </pre> <p>For more information on enabling password-encryption, see <a href="#">password-encryption</a> on page 487.</p> |

alias hashed-string <HASHED-STRING-ALIAS-NAME> <LINE>

hashed-string <HASHED-STRING-ALIAS-NAME>

Creates an alias for a hashed string. Use this alias for configuration values that are hashed strings, such as passwords. For example, in the management-policy, use it to define the privilege mode password. For more information, see [privilege-mode-password](#) on page 1532.

- <HASHED-STRING-ALIAS-NAME> - Specify the hashed-string alias name.

**Note:** Alias name should begin with '\$'.

<LINE>

Configures the hashed-string value associated with this alias.

```
nx9500-6C8809(config)#show running-config
!
alias encrypted-string $WRITE 2
sBqVCDAoxs3oByF5PCSuFAAAAAd7HT2+EiT/1/BXm9c4SBDv
!
alias hashed-string $PriMode 1
faffdde27cb49ad634ea20df4f7c8ef2685894d10ffcb1b2efba054112ecfc75
0
--More--
nx9500-6C8809
```

In the above **show > running-config** output, the '!' displayed before the hashed-string alias value indicates that the displayed text is hashed and not clear text.

alias host <HOST-ALIAS-NAME> <HOST-IP>

host <HOST-ALIAS-NAME>

Creates a host alias, defining a single network host

- <HOST-ALIAS-NAME> - Specify the host alias name.

**Note:** Alias name should begin with '\$'.

<HOST-IP>

Associates the network host's IP address with this host alias. For example, 'alias host \$HOST 1.1.1.100'. In this example, the host alias name is: \$HOST and the host IP address it is mapped to is: 1.1.1.100.

- <HOST-IP> - Specify the network host's IP address.

alias network <NETWORK-ALIAS-NAME> <NETWORK-ADDRESS/MASK>

network  
<NETWORK-ALIAS-NAME>

Creates a network alias, defining a single network address

- <NETWORK-ALIAS-NAME> - Specify the network alias name.

**Note:** Alias name should begin with '\$'.

<NETWORK-ADDRESS/MASK>

Associates a single network with this network alias. For example, 'alias network \$NET 1.1.1.0/24'. In this example, the network alias name is: \$NET and the network it is mapped to is: 1.1.1.0/24.

- <NETWORK-ADDRESS/MASK> - Specify the network's address and mask.

```
alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range <STARTING-IP>
to <ENDING-IP> {<STARTING-IP> to <ENDING-IP>}|host <HOST-IP> {<HOST-IP>}|
network <NETWORK-ADDRESS/MASK> {<NETWORK-ADDRESS/MASK>}]
```

|                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| network <NETWORK-GROUP-ALIAS-NAME>                                        | <p>Creates a network-group alias</p> <ul style="list-style-type: none"> <li>• &lt;NETWORK-GROUP-ALIAS-NAME&gt; – Specify the network-group alias name.</li> </ul> <p><b>Note:</b> Alias name should begin with '\$'.</p> <p>The network-group aliases are used in ACLs, to define the network-specific components. ACLs using aliases can be used across sites by re-defining the network-group alias elements at the device or profile level.</p> <p>After specifying the name, specify the following: a range of IP addresses, host addresses, or a range of network addresses.</p> |
| address-range <STARTING-IP> to <ENDING-IP> {<STARTING-IP> to <ENDING-IP>} | <p>Associates a range of IP addresses with this network-group alias</p> <ul style="list-style-type: none"> <li>• &lt;STARTING-IP&gt; – Specify the first IP address in the range.</li> <li>• to &lt;ENDING-IP&gt; – Specify the last IP address in the range.</li> <li>• &lt;STARTING-IP&gt; to &lt;ENDING-IP&gt; – Optional. Specifies more than one range of IP addresses. A maximum of eight (8) IP address ranges can be configured.</li> </ul>                                                                                                                                   |
| host <HOST-IP> {<HOST-IP>}                                                | <p>Associates a single or multiple hosts with this network-group alias</p> <ul style="list-style-type: none"> <li>• &lt;HOST-IP&gt; – Specify the hosts' IP address.</li> <li>• &lt;HOST-IP&gt; – Optional. Specifies more than one host. A maximum of eight (8) hosts can be configured.</li> </ul>                                                                                                                                                                                                                                                                                  |
| network <NETWORK-ADDRESS/MASK> {<NETWORK-ADDRESS/MASK>}                   | <p>Associates a single or multiple networks with this network-group alias</p> <ul style="list-style-type: none"> <li>• &lt;NETWORK-ADDRESS/MASK&gt; – Specify the network's address and mask.</li> <li>• &lt;NETWORK-ADDRESS/MASK&gt; – Optional. Specifies more than one network. A maximum of eight (8) networks can be configured.</li> </ul>                                                                                                                                                                                                                                      |

```
alias network-service <NETWORK-SERVICE-ALIAS-NAME> proto [<0-254>|<WORD>|eigrp|gre|
igmp|igp|ospf|vrrp] {(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|
ntp|pop3|proto|sip|smtp|sourceport [<1-65535>|<WORD>]|ssh|telnet|tftp|www)}
```

|                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>alias network-service &lt;NETWORK-SERVICE-ALIAS- NAME&gt;</pre>                                                                                                                    | <p>Configures an alias that specifies available network services and the corresponding source and destination software ports</p> <ul style="list-style-type: none"> <li>• &lt;NETWORK-SERVICE-ALIAS-NAME&gt; – Specify a network-service alias name.</li> </ul> <p><b>Note:</b> Alias name should begin with '\$'.</p> <p>Network-service aliases are used in ACLs, to define the service-specific components. ACLs using aliases can be used across sites by re-defining the network-service alias elements at the device or profile level.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <pre>proto [&lt;0-254&gt;  &lt;WORD&gt; eigrp  gre  igmp igp ospf vrrp]</pre>                                                                                                           | <p>Use one of the following options to associate an Internet protocol with this network-service alias:</p> <ul style="list-style-type: none"> <li>• &lt;0-254&gt; – Identifies the protocol by its number. Specify the protocol number from 0 - 254. This is the number by which the protocol is identified in the Protocol field of the IPv4 header and the Next Header field of IPv6 header. For example, the UDP (User Datagram Protocol) designated number is 17.</li> <li>• &lt;WORD&gt; – Identifies the protocol by its name. Specify the protocol name.</li> <li>• eigrp – Selects EIGRP (Enhanced Interior Gateway Routing Protocol). The protocol number 88.</li> <li>• gre – Selects GRE (Generic Routing Encapsulation). The protocol number is 47.</li> <li>• igmp – Selects IGMP (Internet Group Management Protocol). The protocol number is 2.</li> <li>• igp – Selects IGP (Interior Gateway Protocol). The protocol number is 9.</li> <li>• ospf – Selects OSPF (Open Shortest Path First). The protocol number is 89.</li> <li>• vrrp – Selects VRRP (Virtual Router Redundancy Protocol). The protocol number is 112.</li> </ul>                                                                                                                                 |
| <pre>{{(&lt;1-65535&gt;  &lt;WORD&gt;  bgp dns  ftp ftp-data  gopher https ldap  nntp ntp pop3 proto  sip smtp  sourceport [&lt;1-65535&gt;  &lt;WORD&gt;] ssh telnet  tftp www}}</pre> | <p>After specifying the protocol, you may configure a destination port for this service. These keywords are recursive and you can configure multiple protocols and associate multiple destination and source ports.</p> <ul style="list-style-type: none"> <li>• &lt;1-65535&gt; – Optional. Configures a destination port number from 1 - 65535</li> <li>• &lt;WORD&gt; – Optional. Identifies the destination port by the service name provided. For example, the SSH service uses TCP port 22.</li> <li>• bgp – Optional. Configures the default BGP (Border Gateway Protocol) services port (179)</li> <li>• dns – Optional. Configures the default DNS (Domain Name System) services port (53)</li> <li>• ftp – Optional. Configures the default FTP (File Transfer Protocol) control services port (21)</li> <li>• ftp-data – Optional. Configures the default FTP data services port (20)</li> <li>• gopher – Optional. Configures the default gopher services port (70)</li> <li>• https – Optional. Configures the default HTTPS services port (443)</li> <li>• ldap – Optional. Configures the default LDAP (Lightweight Directory Access Protocol) services port (389)</li> <li>• nntp – Optional. Configures the default Newsgroup (NNTP) services port (119)</li> </ul> |



- ntp – Optional. Configures the default NTP (Network Time Protocol) services port (123)
- POP3 – Optional. Configures the default POP3 (Post Office Protocol) services port (110)
- proto – Optional. Use this option to select another Internet protocol in addition to the one selected in the previous step.
- sip – Optional. Configures the default SIP (Session Initiation Protocol) services port (5060)
- smtp – Optional. Configures the default SMTP (Simple Mail Transfer Protocol) services port (25)
- sourceport [<1-65535>|<WORD>] – Optional. After specifying the destination port, you may specify a single or range of source ports.
- <1-65535> – Specify the source port from 1 - 65535.
- <WORD> – Specify the source port range, for example 1-10.
- ssh – Optional. Configures the default SSH services port (22)
- telnet – Optional. Configures the default Telnet services port (23)
- tftp – Optional. Configures the default TFTP (Trivial File Transfer Protocol) services port (69)
- www – Optional. Configures the default HTTP services port (80)

`alias number <NUMBER-ALIAS-NAME> <0-4294967295>`

`alias number <NUMBER-ALIAS-NAME>  
<0-4294967295>`

Creates a number alias identified by the <NUMBER-ALIAS-NAME> keyword. Number aliases map a name to a numeric value. For example, *'alias number \$NUMBER 100'*. In this example:

- The number alias name is: *\$NUMBER*
- The value assigned is: *100*

The value referenced by alias \$NUMBER, wherever used, is 100.

- <NUMBER-ALIAS-NAME> – Specify the number alias name.

**Note:** Alias name should begin with '\$'.

- <0-4294967295> – Specify the number, from 0 - 4294967295, assigned to the number alias created.

`alias string <STRING-ALIAS-NAME> <LINE>`

|                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>alias string &lt;STRING-ALIAS-NAME&gt;</pre> | <p>Creates a string alias identified by the &lt;STRING-ALIAS-NAME&gt; keyword</p> <ul style="list-style-type: none"> <li>• &lt;STRING-ALIAS-NAME&gt; – Specify the string alias name.</li> </ul> <p><b>Note:</b> Alias name should begin with '\$'.</p> <ul style="list-style-type: none"> <li>• &lt;LINE&gt; – Specify the string value.</li> </ul> <p>String aliases map a name to an arbitrary string value. For example, 'alias string \$DOMAIN test.example_company.com'. In this example,</p> <ul style="list-style-type: none"> <li>• the string alias name is: \$DOMAIN</li> <li>• the string value it is mapped to is: test.example_company.com (a domain name).</li> </ul> <p>The value referenced by alias \$DOMAIN, wherever used, is test.example_company.com. You can also use a string alias to configure the Bonjour Service instance name. Once configured, use the string alias in the Bonjour Gateway Discovery Policy context to specify the Bonjour service instance name to be used as the match criteria. For more information, see <a href="#">bonjour-gw-discovery-policy</a> on page 287.</p> |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
alias vlan <VLAN-ALIAS-NAME> <1-4094>
```

|                                               |                                                                                                                                                                                                                                                 |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>alias vlan &lt;VLAN-ALIAS-NAME&gt;</pre> | <p>Creates a VLAN alias identified by the &lt;VLAN-ALIAS-NAME&gt; keyword</p> <ul style="list-style-type: none"> <li>• &lt;VLAN-ALIAS-NAME&gt; – Specify the VLAN alias name.</li> </ul> <p><b>Note:</b> Alias name should begin with '\$'.</p> |
| <pre>&lt;1-4094&gt;</pre>                     | <p>Maps the VLAN alias to a VLAN ID</p> <ul style="list-style-type: none"> <li>• &lt;1-4094&gt; – Specify the VLAN ID from 1 - 4094.</li> </ul>                                                                                                 |

## Examples

```
rfs4000-229D58(config)#alias address-range $TestAddRanAlias 192.168.13.10 to 192.168.13.13
rfs4000-229D58(config)#alias network $TestNetworkAlias 192.168.13.0/24
rfs4000-229D58(config)#alias host $TestHostAlias 192.168.13.100
rfs4000-229D58(config)#alias vlan $TestVLANAlias 1
rfs4000-229D58(config)#alias address-range $AddRangeAlias 192.168.13.2 to 192.168.13.10
rfs4000-229D58(config)#alias network-service $NetServAlias proto igmp
rfs4000-229D58(config)#show running-config | include alias
alias network-group $NetGrAlias address-range 192.168.13.7 to 192.168.13.9 192.168.13.20
to 192.168.13.25
alias network $NetworkAlias 192.168.13.0/24
alias host $HostAlias 192.168.13.10
alias address-range $AddRangeAlias 192.168.13.2 to 192.168.13.10
alias network-service $NetServAlias proto igmp
alias vlan $VlanAlias 1
rfs4000-229D58(config)#
nx9500-6C8809(config)#alias number $NUMBER 100
nx9500-6C8809(config)#show context include-factory | include alias
alias string $DOMAIN test.examplecompany.com
alias string $DOMAIN2 test.example_company.com
alias number $NUMBER 100
alias string $SN B4C7996C8809
nx9500-6C8809(config)#
```

The following examples show encrypted-string alias configuration:

```
nx9500-6C8809(config)#alias encrypted-string $WRITE 0 private
nx9500-6C8809(config)#alias encrypted-string $READ 0 public
nx9500-6C8809(config)#show context | include alias
alias vlan $BLR-01 1
alias string $IN-Blr-EcoSpace-Floor-4 IBEF4
alias encrypted-string $READ 0 public
```

```
alias encrypted-string $WRITE 0 private
nx9500-6C8809(config)#
```

The following example shows the encrypted-string aliases, configured in the previous example, used in the management-policy:

```
nx9500-6C8809(config-management-policy-default)#snmp-server community 0 $WRITE rw
nx9500-6C8809(config-management-policy-default)#snmp-server community 0 $READ ro
nx9500-6C8809(config-management-policy-default)#show context
management-policy default
 no telnet
 no http server
 https server
 rest-server
 ssh
 user admin password 1 ad4d8797f007444ccdda3788b9ee0e8b46f3facb4308e045239eb7771e127ed5
 role superuser access all
 snmp-server community 0 $WRITE rw
 snmp-server community 0 $READ ro
 snmp-server user snmptrap v3 encrypted des auth md5 2 yqr96yyVzmD4ZbU2I7Eh/
 QAAAAjWNKa4KXF95pruUCSnhOiT
 snmp-server user snmpmanager v3 encrypted des auth md5 2 NOF8+2+AY2r4ZbU2I7Eh/
 QAAAAGc018ahJYo3AjHo9wXzYGo
 t5 snmp-server community public ro 192.168.0.1
 t5 snmp-server community private rw 192.168.0.1
nx9500-6C8809(config-management-policy-default)#
```

The following example shows hashed-string alias configuration:

```
nx9500-6C8809(config)#alias hashed-string $PriMode Test12345
nx9500-6C8809(config)#show context | include alias
alias vlan $BLR-01 1
alias string $IN-Blr-EcoSpace-Floor-4 IBEF4
alias encrypted-string $READ 0 public
alias encrypted-string $WRITE 0 private
alias hashed-string $PriMode 1
faffdde27cb49ad634ea20df4f7c8ef2685894d10ffcb1b2efba054112ecfc75
nx9500-6C8809(config)#
```

The following example shows the hashed-string alias, configured in the previous example, used in the management-policy:

```
nx9500-6C8809(config-management-policy-default)#show context
management-policy default
 https server
 rest-server
 ssh
 user admin password 1 ad4d8797f007444ccdda3788b9ee0e8b46f3facb4308e045239eb7771e127ed5
 role superuser access all
 snmp-server community 0 $WRITE rw
 snmp-server community 0 $READ ro
 snmp-server user snmptrap v3 encrypted des auth md5 2 yqr96yyVzmD4ZbU2I7Eh/
 QAAAAjWNKa4KXF95pruUCSnhOiT
 snmp-server user snmpmanager v3 encrypted des auth md5 2 NOF8+2+AY2r4ZbU2I7Eh/
 QAAAAGc018ahJYo3AjHo9wXzYGo
 t5 snmp-server community public ro 192.168.0.1
 t5 snmp-server community private rw 192.168.0.1
 privilege-mode-password $PriMode
nx9500-6C8809(config-management-policy-default)#
```

## Related Commands

|    |                                                             |
|----|-------------------------------------------------------------|
| no | Removes an existing network, VLAN, service, or string alias |
|----|-------------------------------------------------------------|

## ap6522

Adds an AP 6522 to the network. If a profile for the AP is not available, a new profile is created.

### Supported in the following platforms:

- Access Point — AP 6522
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

### Syntax

```
ap6522 <MAC>
```

### Parameters

```
ap6522 <MAC>
```

|       |                                    |
|-------|------------------------------------|
| <MAC> | Specify the AP 6522's MAC address. |
|-------|------------------------------------|

### Examples

```
nx9500-6C8809(config)#ap6522 B4-C7-99-58-72-58
nx9500-6C8809(config-device-B4-C7-99-58-72-58)#show context
ap6522 B4-C7-99-58-72-58
 use profile default-ap6522
 use rf-domain default
 hostname ap6522-587258
nx9500-6C8809(config-device-B4-C7-99-58-72-58)#
nx9500-6C8809(config)#show wireless ap configured
```

| IDX | NAME          | MAC               | PROFILE        | RF-DOMAIN | ADOPTED-BY        |
|-----|---------------|-------------------|----------------|-----------|-------------------|
| 1   | ap6522-587258 | B4-C7-99-58-72-58 | default-ap6522 | default   | B4-C7-99-6C-88-09 |

```
nx9500-6C8809(config)#
```

### Related Commands

|    |                                     |
|----|-------------------------------------|
| no | Removes an AP 6522 from the network |
|----|-------------------------------------|

## ap6562

Adds an AP 6562 to the network. If a profile for the AP is not available, a new profile is created.

### Supported in the following platforms:

- Access Point — AP 6562
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

### Syntax

```
ap6562 <MAC>
```

### Parameters

```
ap6562 <MAC>
```

<MAC> Specify the AP 6562's MAC address.

### Examples

```
nx9500-6C8809(config)#ap6562 00-23-68-31-16-59
nx9500-6C8809(config-device-B4-C7-99-58-72-58)#show context
ap6562 00-23-68-31-16-59
 use profile default-ap6562
 use rf-domain default
 hostname ap6562-311659
nx9500-6C8809(config-device-00-23-68-31-16-59)#
nx9500-6C8809(config)#show wireless ap configured
```

```

 IDX NAME MAC PROFILE RF-DOMAIN ADOPTED-BY

 1 ap6522-587258 B4-C7-99-58-72-58 default-ap6522 default B4-C7-99-6C-88-09
 2 ap6562-311659 00-23-68-31-16-59 default-ap6562 default B4-C7-99-6C-88-09

```

```
nx9500-6C8809(config)#
```

### Related Commands

**no** Removes an AP 6562 from the network

## ap7161

Adds an AP 7161 series to the network. If a profile for the AP is not available, a new profile is created.

### Supported in the following platforms:

- Access Point — AP 7161
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

### Syntax

```
ap71xx <MAC>
```

### Parameters

```
ap71xx <MAC>
```

<MAC> Specify the AP 7161's MAC address.

### Examples

```
nx9500-6C8809(config)#ap71xx 00-23-68-11-E6-C4
nx9500-6C8809(config-device-00-23-68-11-E6-C4)#show context
ap71xx 00-23-68-11-E6-C4
 use profile default-ap71xx
 use rf-domain TechPubs
 hostname ap7161-11E6C4
 no staging-config-learnt
 ip default-gateway 192.168.13.2
 interface vlan1
 ip address 192.168.13.23/24
 use auto-provisioning-policy TecPubs
 no auto-learn staging-config
```

```

adopter-auto-provisioning-policy-lookup evaluate-always
nx9500-6C8809(config-device-00-23-68-11-E6-C4)#
nx9500-6C8809(config)#show wireless ap configured

```

| IDX | NAME          | MAC               | PROFILE        | RF-DOMAIN | ADOPTED-BY        |
|-----|---------------|-------------------|----------------|-----------|-------------------|
| 1   | ap6522-587258 | B4-C7-99-58-72-58 | default-ap6522 | default   | B4-C7-99-6C-88-09 |
| 2   | ap6562-311659 | 00-23-68-31-16-59 | default-ap6562 | default   | B4-C7-99-6C-88-09 |
| 3   | ap7161-11E6C4 | 00-23-68-11-E6-C4 | default-ap71xx | default   | B4-C7-99-6C-88-09 |

```
nx9500-6C8809(config)#
```

### Related Commands

|           |                                     |
|-----------|-------------------------------------|
| <b>no</b> | Removes an AP 7161 from the network |
|-----------|-------------------------------------|

### ap7502

Adds an AP 7502 to the network. If a profile for the AP is not available, a new profile is created.

### Supported in the following platforms:

- Access Point — AP 7502
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

### Syntax

```
ap7502 <MAC>
```

### Parameters

```
ap7502 <MAC>
```

|       |                                    |
|-------|------------------------------------|
| <MAC> | Specify the AP 7502's MAC address. |
|-------|------------------------------------|

### Examples

```

rfs4000-6DB5D4(config)#ap7502 00-23-68-99-BF-A8
rfs4000-6DB5D4(config-device-00-23-68-99-BF-A8)#show context
ap7502 00-23-68-99-BF-A8
 use profile default-ap7502
 use rf-domain default
 hostname ap7502-99BFA8
 mint mlcp vlan
 mint mlcp ip
 use radius-server-policy eap
 interface radiol
 rf-mode 2.4GHz-wlan
 wlan open_test bss 1 primary
 interface radio2
 rf-mode 5GHz-wlan
 wlan open_test bss 1 primary
rfs4000-6DB5D4(config-device-00-23-68-99-BF-A8)#
rfs4000-6DB5D4(config)#show wireless ap configured

```

| IDX | NAME          | MAC               | PROFILE        | RF-DOMAIN | ADOPTED-BY        |
|-----|---------------|-------------------|----------------|-----------|-------------------|
| 1   | ap7502-99BFA8 | 00-23-68-99-BF-A8 | default-ap7502 | default   | 00-15-70-6D-B5-D4 |

```
rfs4000-6DB5D4(config)#
```

## Related Commands

|                 |                                     |
|-----------------|-------------------------------------|
| <code>no</code> | Removes an AP 7502 from the network |
|-----------------|-------------------------------------|

### *ap7522*

Adds an AP 7502 to the network. If a profile for the AP is not available, a new profile is created.

#### Supported in the following platforms:

- Access Point — AP 7522
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

#### Syntax

`ap7522 <MAC>`

#### Parameters

`ap7522 <MAC>`

|                          |                                    |
|--------------------------|------------------------------------|
| <code>&lt;MAC&gt;</code> | Specify the AP 7522's MAC address. |
|--------------------------|------------------------------------|

#### Examples

```
NOC-NX9500(config)#ap7522 84-24-8D-83-30-A4
NOC-NX9500(config-device-84-24-8D-83-30-A4)#show context
ap7522 84-24-8D-83-30-A4
 use profile default-ap7522
 use rf-domain default
 hostname ap7522-8330A4
 mint mlcp vlan
 mint mlcp ip
 use radius-server-policy eap
 interface radio1
 rf-mode 2.4GHz-wlan
 wlan open_test bss 1 primary
 interface radio2
 rf-mode 5GHz-wlan
 wlan open_test bss 1 primary
NOC-NX9500(config-device-84-24-8D-83-30-A4)#
NOC-NX9500(config)#show wireless ap configured
```

| IDX | NAME          | MAC               | PROFILE        | RF-DOMAIN | ADOPTED-BY        |
|-----|---------------|-------------------|----------------|-----------|-------------------|
| 1   | ap7522-8330A4 | 84-24-8D-83-30-A4 | default-ap7522 | default   | B4-C7-99-6C-88-09 |
| 2   | ap8163-74B45C | B4-C7-99-74-B4-5C | default-ap81xx | default   | B4-C7-99-6C-88-09 |

```
NOC-NX9500(config)#
```

#### Related Commands

|                 |                                     |
|-----------------|-------------------------------------|
| <code>no</code> | Removes an AP 7522 from the network |
|-----------------|-------------------------------------|

### *ap7532*

Adds an AP 7532 to the network. If a profile for the AP is not available, a new profile is created.

### Supported in the following platforms:

- Access Point — AP 7532
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

### Syntax

```
ap7532 <MAC>
```

### Parameters

```
ap7532 <MAC>
```

|       |                                    |
|-------|------------------------------------|
| <MAC> | Specify the AP 7532's MAC address. |
|-------|------------------------------------|

### Examples

```
rfs4000-6DB5D4(config)#ap7532 00-23-68-12-B6-18
rfs4000-6DB5D4(config-device-00-23-68-12-B6-18)#show context
ap7532 00-23-68-12-B6-18
 use profile default-ap7532
 use rf-domain default
 hostname ap7532-12B618
 mint mlcp vlan
 mint mlcp ip
 use radius-server-policy eap
 interface radio1
 rf-mode 2.4GHz-wlan
 wlan open bss 1 primary
 interface radio2
 rf-mode 5GHz-wlan
 wlan open bss 1 primary
rfs4000-6DB5D4(config-device-00-23-68-12-B6-18)#
rfs4000-6DB5D4(config)#show wireless ap configured
```

| IDX | NAME          | MAC               | PROFILE        | RF-DOMAIN | ADOPTED-BY        |
|-----|---------------|-------------------|----------------|-----------|-------------------|
| 1   | ap7502-99BFA8 | 00-23-68-99-BF-A8 | default-ap7502 | default   | 00-15-70-6D-B5-D4 |
| 2   | ap7532-12B618 | 00-23-68-12-B6-18 | default-ap7532 | default   | 00-15-70-6D-B5-D4 |

```
rfs4000-6DB5D4(config)#
```

### Related Commands

|    |                                     |
|----|-------------------------------------|
| no | Removes an AP 7532 from the network |
|----|-------------------------------------|

### ap7562

Adds an AP 7562 series to the network. If a profile for the AP is not available, a new profile is created.

### Supported in the following platforms:

- Access Point — AP 7562
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

### Syntax

```
ap7562 <MAC>
```



## Parameters

ap7562 <MAC>

|       |                                    |
|-------|------------------------------------|
| <MAC> | Specify the AP 7562's MAC address. |
|-------|------------------------------------|

## Examples

```
rfs4000-6DB5D4(config)#ap7562 01-16-71-A1-CD-20
rfs4000-6DB5D4(config-device-01-16-71-A1-CD-20)#show context
```

```
ap7562 01-16-71-A1-CD-20
 use profile default-ap7562
 use rf-domain default
 hostname ap7562-A1CD20
 mint mlcp vlan
 mint mlcp ip
 use radius-server-policy eap
 interface radiol
 rf-mode 2.4GHz-wlan
 wlan open bss 1 primary
 interface radio2
 rf-mode 5GHz-wlan
 wlan open bss 1 primary
```

```
rfs4000-6DB5D4(config-device-01-16-71-A1-CD-20)#
rfs4000-6DB5D4(config)#show wireless ap configured
```

| IDX | NAME          | MAC               | PROFILE        | RF-DOMAIN | ADOPTED-BY        |
|-----|---------------|-------------------|----------------|-----------|-------------------|
| 1   | ap7502-99BFA8 | 00-23-68-99-BF-A8 | default-ap7502 | default   | 00-15-70-6D-B5-D4 |
| 2   | ap7532-12B618 | 00-23-68-12-B6-18 | default-ap7532 | default   | 00-15-70-6D-B5-D4 |
| 3   | ap7562-A1CD20 | 01-16-71-A1-CD-20 | default-ap7562 | default   | 00-15-70-6D-B5-D4 |

```
rfs4000-6DB5D4(config)#
```

## Related Commands

|    |                                     |
|----|-------------------------------------|
| no | Removes an AP 7562 from the network |
|----|-------------------------------------|

ap7602

Adds an AP 7602 to the network. If a profile for the AP is not available, a new profile is created.

## Supported in the following platforms:

- Access Point — AP 7602
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

## Syntax

ap7602 <MAC>

## Parameters

ap7602 <MAC>

|       |                                    |
|-------|------------------------------------|
| <MAC> | Specify the AP 7602's MAC address. |
|-------|------------------------------------|

## Examples

```
nx9500-6C8809(config)#ap7602 11-2C-3b-01-AA-23
nx9500-6C8809(config-device-11-2C-3b-01-AA-23)#show context
ap7602 11-2C-3b-01-AA-233
 use profile default-ap7602
 use rf-domain default
 hostname ap7602-01AA23
nx9500-6C8809(config-device-11-2C-3b-01-AA-23)#
```

## Related Commands

|                 |                                     |
|-----------------|-------------------------------------|
| <code>no</code> | Removes an AP 7602 from the network |
|-----------------|-------------------------------------|

### *ap7612*

Adds an AP 7612 to the network. If a profile for the AP is not available, a new profile is created.

#### Supported in the following platforms:

- Access Point — AP 7612
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
ap7612 <MAC>
```

#### Parameters

```
ap7612 <MAC>
```

|                          |                                    |
|--------------------------|------------------------------------|
| <code>&lt;MAC&gt;</code> | Specify the AP 7612's MAC address. |
|--------------------------|------------------------------------|

## Examples

```
nx9500-6C8809(config)#ap7612 10-1c-AB-11-0E-20
nx9500-6C8809(config-device-10-1c-AB-11-0E-20)#show context
ap7612 10-1C-AB-11-0E-20
 use profile default-ap7612
 use rf-domain default
 hostname ap7612-110E20
nx9500-6C8809(config-device-10-1c-AB-11-0E-20)#
```

## Related Commands

|                 |                                     |
|-----------------|-------------------------------------|
| <code>no</code> | Removes an AP 7612 from the network |
|-----------------|-------------------------------------|

### *ap7622*

Adds an AP 7622 to the network. If a profile for the AP is not available, a new profile is created.

#### Supported in the following platforms:

- Access Point — AP 7622
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

## Syntax

```
ap7622 <MAC>
```

## Parameters

```
ap7622 <MAC>
```

|       |                                    |
|-------|------------------------------------|
| <MAC> | Specify the AP 7622's MAC address. |
|-------|------------------------------------|

## Examples

```
nx9500-6C8809(config)#ap7622 01-11-CD-21-0B-13
nx9500-6C8809(config-device-01-11-CD-21-0B-13)#show con
ap7622 01-11-CD-21-0B-13
 use profile default-ap7622
 use rf-domain default
 hostname ap7622-210B13
nx9500-6C8809(config-device-01-11-CD-21-0B-13)#
```

## Related Commands

|           |                                     |
|-----------|-------------------------------------|
| <b>no</b> | Removes an AP 7622 from the network |
|-----------|-------------------------------------|

## ap7632

Adds an AP 7632 to the network. If a profile for the AP is not available, a new profile is created.

### Supported in the following platforms:

- Access Point — AP 7632
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

## Syntax

```
ap7632 <MAC>
```

## Parameters

```
ap7632 <MAC>
```

|       |                                    |
|-------|------------------------------------|
| <MAC> | Specify the AP 7632's MAC address. |
|-------|------------------------------------|

## Examples

```
nx9500-6C8809(config)#ap7632 23-12-A1-F0-12-02
nx9500-6C8809(config-device-23-12-A1-F0-12-02)#show context
ap7632 23-12-A1-F0-12-02
 use profile default-ap7632
 use rf-domain default
 hostname ap7632-F01202
nx9500-6C8809(config-device-23-12-A1-F0-12-02)#
```

## Related Commands

|           |                                     |
|-----------|-------------------------------------|
| <b>no</b> | Removes an AP 7662 from the network |
|-----------|-------------------------------------|

## ap7662

Adds an AP 7662 to the network. If a profile for the AP is not available, a new profile is created.

### Supported in the following platforms:

- Access Point — AP 7662
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

### Syntax

```
ap7662 <MAC>
```

### Parameters

```
ap7662 <MAC>
```

|       |                                    |
|-------|------------------------------------|
| <MAC> | Specify the AP 7662's MAC address. |
|-------|------------------------------------|

### Examples

```
nx9500-6C8809(config)#ap7662 20-12-bd-4C-31-5F
nx9500-6C8809(config-device-20-12-BD-4C-31-5F)#show context
ap7662 20-12-BD-4C-31-5F
 use profile default-ap7662
 use rf-domain default
 hostname ap7662-4C315F
nx9500-6C8809(config-device-20-12-BD-4C-31-5F)#
```

### Related Commands

|    |                                     |
|----|-------------------------------------|
| no | Removes an AP 7662 from the network |
|----|-------------------------------------|

## ap8163

Adds an AP 8163 series to the network. If a profile for the AP is not available, a new profile is created.

### Supported in the following platforms:

- Access Point — AP 8163
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

### Syntax

```
ap81xx <MAC>
```

### Parameters

```
ap81xx <MAC>
```

|       |                                    |
|-------|------------------------------------|
| <MAC> | Specify the AP 8163's MAC address. |
|-------|------------------------------------|

### Examples

```
rfs4000-6DB5D4#ap81xx B4-C7-99-71-17-28
rfs4000-6DB5D4(config-device-B4-C7-99-71-17-28)#show context
ap81xx B4-C7-99-71-17-28
```

```

use profile default-ap81xx
use rf-domain default
hostname ap8163-711728
license AAP DEFAULT-LICENSE
rfs4000-6DB5D4(config-device-B4-C7-99-71-17-28)#
rfs4000-6DB5D4(config)#show wireless ap configured

```

```

IDX NAME MAC PROFILE RF-DOMAIN ADOPTED-BY

1 ap8163-711728 B4-C7-99-71-17-28 default-ap81xx default 00-15-70-6D-B5-D4

rfs4000-6DB5D4(config)#

```

### Related Commands

|           |                                     |
|-----------|-------------------------------------|
| <b>no</b> | Removes an AP 8163 from the network |
|-----------|-------------------------------------|

### ap8432

Adds an AP 8432 to the network. If a profile for the AP is not available, a new profile is created.

### Supported in the following platforms:

- Access Point — AP 8432
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

### Syntax

```
ap8432 <MAC>
```

### Parameters

```
ap8432 <MAC>
```

|       |                                    |
|-------|------------------------------------|
| <MAC> | Specify the AP 8432's MAC address. |
|-------|------------------------------------|

### Examples

```

nx9500-6C8809(config)#ap8432 84-24-8D-80-C2-AC
nx9500-6C8809(config-device-84-24-8D-80-C2-AC)#show context
ap8432 84-24-8D-80-C2-AC
 use profile default-ap8432
 use rf-domain default
 hostname ap8432-80C2AC
nx9500-6C8809(config-device-84-24-8D-80-C2-AC)#
nx9500-6C8809(config)#show wireless ap configured

```

```

IDX NAME MAC PROFILE RF-DOMAIN ADOPTED-BY

1 ap8432-80C2AC 84-24-8D-80-C2-AC default-ap8432 default un-adopted

nx9500-6C8809(config)#

```

### Related Commands

|           |                             |
|-----------|-----------------------------|
| <b>no</b> | Removes an from the network |
|-----------|-----------------------------|

## ap8533

Adds an AP 8533 to the network. If a profile for the AP is not available, a new profile is created.

### Supported in the following platforms:

- Access Point — AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

### Syntax

```
ap8533 <MAC>
```

### Parameters

```
ap8533 <MAC>
```

|       |                                    |
|-------|------------------------------------|
| <MAC> | Specify the AP 8533's MAC address. |
|-------|------------------------------------|

### Examples

```
nx9500-6C8809(config)#ap8533 B4-C7-99-74-B4-5C
nx9500-6C8809(config-device-B4-C7-99-74-B4-5C)#show context
ap8533 B4-C7-99-74-B4-5C
 use profile default-ap8533
 use rf-domain default
 hostname ap8533-74B45C
nx9500-6C8809(config-device-B4-C7-99-74-B4-5C)#
nx9500-6C8809(config)#show wireless ap configured
```

| IDX | NAME          | MAC               | PROFILE        | RF-DOMAIN | ADOPTED-BY |
|-----|---------------|-------------------|----------------|-----------|------------|
| 1   | ap8533-74B45C | B4-C7-99-74-B4-5C | default-ap8533 | default   | un-adopted |

```
nx9500-6C8809(config)#
```

### Related Commands

|    |                                     |
|----|-------------------------------------|
| no | Removes an AP 8533 from the network |
|----|-------------------------------------|

## application

Creates a new application definition and enters its configuration mode. Use this command to create a customized application detection definition.

### Supported in the following platforms:

- Access Points — AP 7522, AP 7532
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

### Syntax

```
application <APPLICATION-NAME>
```

### Parameters

```
application <APPLICATION-NAME>
```

|                                |                                                                                                                                                                                     |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| application <APPLICATION-NAME> | Creates a new application definition and enters its configuration mode                                                                                                              |
|                                | <ul style="list-style-type: none"> <li>&lt;APPLICATION-NAME&gt; – Specify a name of the new application definition. It is created if not already existing in the system.</li> </ul> |

### Examples

```

nx9500-6C8809(config)#application Bing
nx9500-6C8809(config-application-Bing)#?
Application Mode commands:
 app-category Set application category (default is custom)
 description Add application description
 https Secure HTTP
 no Negate a command or set its defaults
 use Set setting to use

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-application-Bing)#

```

### Related Commands

|                         |                                                        |
|-------------------------|--------------------------------------------------------|
| no (global-config-mode) | Removes an existing application definition on page 475 |
|-------------------------|--------------------------------------------------------|

### application-mode-commands

The following table summarizes Application definition configuration mode commands:

**Table 7: Application Config Mode Commands**

| Command                                            | Description                                                                                                                                                |
|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| app-category (application-config-mode) on page 259 | Configures the category for this application definition                                                                                                    |
| description (application-config-mode) on page 260  | Configures a description for this application definition                                                                                                   |
| https (application-config-mode) on page 261        | Configures the HTTPS common-name attribute value for this application category's server certificate. Applicable only to applications using HTTPS protocol. |
| use (application-config-mode) on page 261          | Associates a network-service alias or a URL list with this application definition. Applicable for applications using protocols other than HTTPS.           |
| no (application-config-mode) on page 262           | Removes or resets this application definition's configured settings                                                                                        |

app-category (application-config-mode)

Configures the category for this application definition

Supported in the following platforms:

- Access Points — AP 7522, AP 7532
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
app-category <APP-CATEGORY-NAME>
```

#### Parameters

```
app-category <APP-CATEGORY-NAME>
```

|                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| app-category <APP-CATEGORY-NAME> | Select the category best suited for this application definition. There are twenty three categories. These are: business, conference, custom, database, filetransfer, gaming, generic, im, mail, mobile, network\ management, other, p2p, remote_control, social\ networking, standard, streaming, tunnel, video, voip, and Web.<br>The default setting is custom. Use this option to categorize your internal custom applications, so that they do not appear as unknown traffic. |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config-application-Bing)#app-category [TAB]
business conference custom
database filetransfer gaming
generic im mail
mobile network\ management other
p2p remote_control sharehosting
social\ networking streaming tunnel
voip web
```

```
nx9500-6C8809(config-application-Bing)#
nx9500-6C8809(config-application-Bing)#app-category streaming
nx9500-6C8809(config-application-Bing)#show context
application Bing
 app-category streaming
nx9500-6C8809(config-application-Bing)#
```

#### Related Commands

|                                          |                                                 |
|------------------------------------------|-------------------------------------------------|
| no (application-config-mode) on page 262 | Resets application category to default (custom) |
|------------------------------------------|-------------------------------------------------|

description (application-config-mode)

Configures a description for this application definition

Supported in the following platforms:

- Access Points — AP 7522, AP 7532
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
description <WORD>
```

#### Parameters

```
description <WORD>
```

|                    |                                                                                                                                                                                                                              |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| description <WORD> | Configures a description for this application <ul style="list-style-type: none"><li>• &lt;WORD&gt; - Specify a description not exceeding 80 characters in length. Enter the descriptive text within double quotes.</li></ul> |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



## Examples

```
nx9500-6C8809(config-application-Bing)#description "Bing is Microsoft's Web search engine"
nx9500-6C8809(config-application-Bing)#show context
application Bing
 description "Bing is Microsoft's Web search engine"
 app-category streaming
nx9500-6C8809(config-application-Bing)#
```

## Related Commands

|                                                       |                                                          |
|-------------------------------------------------------|----------------------------------------------------------|
| <code>no (application-config-mode)</code> on page 262 | Removes this description configured for this application |
|-------------------------------------------------------|----------------------------------------------------------|

## https (application-config-mode)

Configures the HTTPS parameter type, attribute type, match criteria for the HTTPS server name and 64 character maximum server name attribute used in the HTTPS server message exchange

Supported in the following platforms:

- Access Points — AP 7522, AP 7532
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

## Syntax

```
https server-cert common-name [contains|ends-with] <WORD>
```

## Parameters

```
https server-cert common-name [contains|ends-with] <WORD>
```

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| https server-cert                       | Configures the HTTPS parameter type as server certificate                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| common-name [contains ends-with] <WORD> | Configures the HTTPS attribute match criteria as common name. This is the only option applicable when the HTTPS parameter type is set to server-cert. Use one of the following options to provide the common-name attribute value used as the match criteria: <ul style="list-style-type: none"><li>• contains - Filters applications having common-name attributes containing the string specified here</li><li>• ends-with - Filters applications ending with the string specified here<ul style="list-style-type: none"><li>• &lt;WORD&gt; - Specify the string to match (should not exceed 64 characters).</li></ul></li></ul> |

## Examples

```
nx9500-6C8809(config-application-Bing)#https server-cert common-name exact bing.com
nx9500-6C8809(config-application-Bing)#show context
application Bing
 description "Bing is Microsoft's web search engine"
 app-category streaming
 https server-cert common-name exact bing.com
nx9500-6C8809(config-application-Bing)#
```

## Related Commands

|                                                       |                                                                                         |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------|
| <code>no (application-config-mode)</code> on page 262 | Removes the HTTPS common-name attribute value configured with this application category |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------|

## use (application-config-mode)

Associates a network-service alias or a URL list with this application definition

For applications using protocols other than HTTPS, use this command to define the protocols, ports, and/or URL host name to match.

Supported in the following platforms:

- Access Points — AP 7522, AP 7532
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
use [network-service <NETWORK-SERVICE-ALIAS-NAME>|url-list <URL-LIST-NAME>]
```

#### Parameters

```
use [network-service <NETWORK-SERVICE-ALIAS-NAME>|url-list <URL-LIST-NAME>]
```

|                                              |                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| use                                          | Configures this application definition to use a network-service alias or a URL list                                                                                                                                                                                                                                                                                                                                       |
| network-service <NETWORK-SERVICE-ALIAS-NAME> | Associates a network-service alias with this application definition <ul style="list-style-type: none"><li>• &lt;NETWORK-SERVICE-ALIAS-NAME&gt; - Specify the network-service alias name (should be existing and configured). The network-service alias should specify the protocols and ports to match.</li></ul>                                                                                                         |
| url-list <URL-LIST-NAME>                     | Associates a URL list with this application definition. URL lists are utilized for whitelisting and blacklisting Web application URLs from being launched and consuming bandwidth within the WiNG managed network. <ul style="list-style-type: none"><li>• &lt;URL-LIST-NAME&gt; - Specify the URL list name (should be existing and configured). The URL list should specify the HTTP URL host names to match.</li></ul> |

#### Examples

```
nx9500-6C8809(config-application-Bing)#use url-list Bing
nx9500-6C8809(config-application-Bing)#show context
application Bing
 description "Bing is Microsoft's web search engine"
 app-category streaming
 use url-list Bing
 https server-cert common-name exact bing.com
nx9500-6C8809(config-application-Bing)#
```

#### Related Commands

|                                          |                                                                                               |
|------------------------------------------|-----------------------------------------------------------------------------------------------|
| no (application-config-mode) on page 262 | Removes the network-service alias or the URL list associated with this application definition |
|------------------------------------------|-----------------------------------------------------------------------------------------------|

no (application-config-mode)

Removes or resets this application definition's configured settings

Supported in the following platforms:

- Access Points — AP 7522, AP 7532
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
no [app-category|description|https|use]
no [app-category|description]
no https server-cert common-name [contains|ends-with] <WORD>
no use [network-service <NETWORK-SERVICE-ALIAS-NAME>|url-list <URL-LIST-NAME>]
```

#### Parameters

```
no <PARAMETERS>
```

|                 |                                                                                                    |
|-----------------|----------------------------------------------------------------------------------------------------|
| no <PARAMETERS> | Removes or resets this application definition's configured settings based on the parameters passed |
|-----------------|----------------------------------------------------------------------------------------------------|

Example (User Exec Mode)

Example (Privi Exec Mode)

The following example displays the application definition 'Bing' parameters before the 'no' commands are executed:

```
nx9500-6C8809(config-application-Bing)#show context
application Bing
 description "Bing is Microsoft's web search engine"
 app-category streaming
 use url-list Bing
 https server-cert common-name exact bing.com
nx9500-6C8809config-application-Bing)#
nx9500-6C8809(config-application-Bing)#no description
nx9500-6C8809(config-application-Bing)#no https server-cert common-name exact bing.com
```

The following example displays the application definition 'Bing' parameters after the 'no' commands are executed:

```
nx9500-6C8809(config-application-Bing)#show context
application Bing
 app-category streaming
 use url-list Bing
nx9500-6C8809(config-application-Bing)#
```

### *application-group*

An application group is a collection of system-provided and/or user-defined applications. It is a subset of the total number of supported applications. There are a total of 300 system-provided applications.

WiNG, nx9500-6C8809

#### **Supported in the following platforms:**

- Access Points — AP 7522, AP 7532
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

#### **Syntax**

```
application-group <APPLICATION-GROUP-NAME>
```

#### **Parameters**

```
application-group <APPLICATION-GROUP-NAME>
```

|                                               |                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| application-group<br><APPLICATION-GROUP-NAME> | Creates an application group and enters its configuration mode <ul style="list-style-type: none"> <li>• &lt;APPLICATION-GROUP-NAME - Specify the application group name. If an application group with the specified name does not exist, it is created. The name should not exceed 32 characters in length.</li> </ul> |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### **Examples**

```
nx9500-6C8809(config)#application-group amazon
nx9500-6C8809(config-app-group-amazon)#?
Application Group Mode commands:
 application Add application to group
```

```

description Add application-group description
no Negate a command or set its defaults

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

```

```
nx9500-6C8809(config-app-group-amazon)#
```

### Related Commands

`no (global-config-mode)` Removes an existing application group on page 475

### application-group-mode-commands

The following table summarizes the application group configuration mode commands:

**Table 8: Application Group Config Commands**

| Command                                                              | Description                                                                             |
|----------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| <code>application (application-group-config-mode)</code> on page 264 | Adds an application to this application group                                           |
| <code>description (application-group-config-mode)</code> on page 265 | Configures a description for this application group                                     |
| <code>no (application-group-config-mode)</code> on page 266          | Removes this application group's configured parameters (application and/or description) |

#### application (application-group-config-mode)

Adds an application to this application group. You can add a system-provided or user-defined application.

Supported in the following platforms:

- Access Points — AP 7522, AP 7532
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
application <APPLICATION-NAME>
```

#### Parameters

```
application <APPLICATION-NAME>
```

application <APPLICATION-NAME>

Configures the application to be added to this application group

- <APPLICATION-NAME> - Provide the application name (should be available as an option in the system). A maximum of eight (8) applications can be added to a group.

**Note:** If the desired application is not available as an option, use the `application` command to add it.

## Examples

To view all applications available in the system, use [TAB], as shown in the following example:

```
nx9500-6C8809(config-app-group-test)#application [TAB]
Display all 300 possibilities? (y or n)
1-clickshare-com 1-upload-com
1-upload-to 10upload-com

--More--
nx9500-6C8809(config-app-group-test)#
```

Select the desired application from the list displayed, as shown in the following examples:

```
nx9500-6C8809(config-app-group-amazon)#application amazon [TAB]
amazon-prime-music amazon-prime-video amazon_cloud amazon_shop
nx9500-6C8809(config-app-group-amazon)#
nx9500-6C8809(config-app-group-amazon)#application amazon-prime-music
nx9500-6C8809(config-app-group-amazon)#application amazon-prime-video
nx9500-6C8809(config-app-group-amazon)#application amazon_cloud
nx9500-6C8809(config-app-group-amazon)#application amazon_shop
nx9500-6C8809(config-app-group-amazon)#show context
application-group amazon
 application amazon-prime-music
 application amazon-prime-video
 application amazon_cloud
 application amazon_shop
nx9500-6C8809(config-app-group-amazon)#
```

Note, the system returns an error message if the application entered is not listed, as shown in the following example:

```
nx9500-6C8809(config-app-group-test)#application bing
% Error: application 'bing' is not defined
nx9500-6C8809(config-app-group-test)#
```

## Related Commands

`no (application-group-config-mode)` on page 266

Removes a specified application from this application group

description (application-group-config-mode)

Configures a description for this application group

Supported in the following platforms:

- Access Points — AP 7522, AP 7532
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

## Syntax

description <WORD>

## Parameters

description <WORD>

|                    |                                                                                                                                                                                                                                                          |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| description <WORD> | Configures a description for this application group that uniquely differentiates it from other existing application groups <ul style="list-style-type: none"><li>• &lt;WORD&gt; - Provide a description not exceeding 80 characters in length.</li></ul> |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-app-group-amazon)#description "This application-group lists
all Amazon applications."
nx9500-6C8809(config-app-group-amazon)#show context
application-group amazon
description "This application-group lists all Amazon applications."
application amazon-prime-music
application amazon-prime-video
application amazon_cloud
application amazon_shop
nx9500-6C8809(config-app-group-amazon)#
```

## Related Commands

|                                                |                                                               |
|------------------------------------------------|---------------------------------------------------------------|
| no (application-group-config-mode) on page 266 | Removes the description configured for this application group |
|------------------------------------------------|---------------------------------------------------------------|

## no (application-group-config-mode)

Removes this application group's configured parameters (application and/or description)

Supported in the following platforms:

- Access Points — AP 7522, AP 7532
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

## Syntax

```
no [application <APPLICATION-NAME>|description]
```

## Parameters

```
no [application <APPLICATION-NAME>|description]
```

|                 |                                                                                         |
|-----------------|-----------------------------------------------------------------------------------------|
| no <PARAMETERS> | Removes an application associated with this group, and removes this group's description |
|-----------------|-----------------------------------------------------------------------------------------|

## Examples

The following example displays the application-group 'amazon' configuration before the execution of 'no' commands:

```
nx9500-6C8809(config-app-group-amazon)#show context
application-group amazon
description "This application-group lists all Amazon applications."
application amazon-prime-music
application amazon-prime-video
application amazon_cloud
application amazon_shop
nx9500-6C8809(config-app-group-amazon)#
nx9500-6C8809(config-app-group-amazon)#no application amazon_cloud
nx9500-6C8809(config-app-group-amazon)#no description
```

The following example displays the application-group 'amazon' configuration after the execution of 'no' commands:

```
nx9500-6C8809(config-app-group-amazon)#show context
application-group amazon
 application amazon-prime-music
 application amazon-prime-video
 application amazon_shop
nx9500-6C8809(config-app-group-amazon)#
```

### *application-policy*

When an application is recognized and classified by the WiNG application recognition engine, administrator defined actions can be applied to that specific application. An application policy defines the rules or actions executed on recognized applications (for example, Facebook) or application-categories (for example, social-networking). The following are the rules/actions that can be applied in an application policy:

- *Allow* - Allows packets for a specific application or application category
- *Deny* - Denies packets for a specific application or application category
- *Mark* - Marks packets with DSCP/8021p value for a specific application or application category
- *Rate-limit* - Rate limits packets from specific application types.

For each rule defined, a precedence is assigned to resolve conflicting rules for applications and categories. A *deny* rule is exclusive, as no other action can be combined with a deny. An *allow* rule is redundant with other actions, since the default action is allow. An allow rule is useful when wanting to deny packets for a category, but wanting to allow a few applications in the same category to proceed. In such a cases, add an allow rule for applications with a higher precedence then a deny rule for that category.

*Mark* actions mark packets for a recognized application and category with DSCP/8021p values used for QoS. Rate-limits create a rate-limiter applied to packets recognized for an application and category. Ingress and egress rates need to be specified for the rate-limiter, but both are not required. Mark and rate-limit are the only two actions that can be combined for an application and category. All other combinations are invalid.

Once created and configured, apply the application policy at the following levels within the network to enforce application assurance:

- RADIUS CoA usage - In the device/profile configuration mode, use the **application-policy > radius > <APPLICATION-POLICY-NAME>** command to apply the policy to every user successfully authenticated by the RADIUS server.
- User role - In the role-policy-user-role configuration mode, use the **use > application-policy <APPLICATION-POLICY-NAME>** command to apply the policy to all users assigned to the role.
- WLAN - In the WLAN configuration mode, use the **use > application-policy <APPLICATION-POLICY-NAME>** command to apply the policy to all users accessing the WLAN.
- Bridge VLAN - In the bridge VLAN configuration mode, use the **use > application-policy <APPLICATION-POLICY-NAME>** command to apply the policy for the traffic corresponding to the bridged VLAN.

#### **Supported in the following platforms:**

- Access Points — AP 7522, AP 7532
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

## Syntax

```
application-policy <APPLICATION-POLICY-NAME>
```

## Parameters

```
application-policy <APPLICATION-POLICY-NAME>
```

|                                                 |                                                                                                                                                                          |
|-------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| application-policy<br><APPLICATION-POLICY-NAME> | Specify the application policy name. If an application policy with the specified name does not exist, it is created. The name should not exceed 32 characters in length. |
|-------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config)#application-policy TestAppliPolicy
nx9500-6C8809(config-app-policy-TestAppliPolicy)#?
Application Policy Mode commands:
 allow Allow packets
 deny Deny packets
 description Application policy description
 enforcement-time Configure policy enforcement based on time
 logging Application recognition logging
 mark Mark packets
 no Negate a command or set its defaults
 rate-limit Rate-limit packets

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-app-policy-TestAppliPolicy)#
```

## Related Commands

[no \(global-config-mode\)](#) Removes an existing application policy on page 475

## application-policy-mode-commands

The following table summarizes Application policy configuration mode commands:

**Table 9: Application Policy Config Commands**

| Command                                                                  | Description                                                                                                                      |
|--------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">allow (application-policy-config-mode)</a> on page 269       | Creates an allow rule and configures the match criteria based on which packets are filtered and the allow access action appliedc |
| <a href="#">deny (application-policy-config-mode)</a> on page 272        | Creates a deny rule and configures the match criteria based on which packets are filtered and the deny access action applied     |
| <a href="#">description (application-policy-config-mode)</a> on page 274 | Configures a brief description for this application policy that enables you to differentiate it from other application policies  |



**Table 9: Application Policy Config Commands (continued)**

| Command                                                                    | Description                                                                                                                                                  |
|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>enforcement-time (application-policy-config-mode)</code> on page 275 | Configures an enforcement time period in days and hours for this application policy. The policy is enforced only during the specified time period.           |
| <code>logging (application-policy-config-mode)</code> on page 276          | Enables logging of application recognition hits made by the DPI engine. It also sets the logging level.                                                      |
| <code>mark (application-policy-config-mode)</code> on page 277             | Creates a mark rule and configures the match criteria based on which packets are filtered and marked with 802.1p priority value or DSCP code                 |
| <code>rate-limit (application-policy-config-mode)</code> on page 280       | Creates a rate-limit rule and configures the match criteria based on which incoming and outgoing packets are filtered and the configured rate limits applied |
| <code>no (application-policy-config-mode)</code> on page 282               | Removes or resets this application policy settings                                                                                                           |

### allow (application-policy-config-mode)

Creates an allow rule and configures the match criteria based on which packets are filtered and the allow access action applied

Supported in the following platforms:

- Access Points — AP 7522, AP 7532
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
allow [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>] schedule <SCHEDULE-POLICY-NAME> (precedence <1-256>)
```

#### Parameters

```
allow [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>] schedule <SCHEDULE-POLICY-NAME> (precedence <1-256>)
```

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| allow                                  | Creates an allow rule and configures the match criteria. The options are app-category and application.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| app-category [<APP-CATEGORY-NAME> all] | <p>Uses application category as the match criteria</p> <ul style="list-style-type: none"> <li>• &lt;APP-CATEGORY-NAME&gt; - Specify the application category. The options are: antivirus\ update, audio, business, conference, custom, database, file transfer, gaming, generic, im, mail, mobile, network\ management, other, p2p, remote_control, social\ networking, standard, streaming, tunnel, video, voip, and web. Each packet's app-category is matched with the value specified here. In case of a match, the system forwards the packet or else drops it.</li> <li>• all - The system forwards all packets irrespective of the application category.</li> </ul> |

|                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>application &lt;APPLICATION-NAME&gt;</p>  | <p>Uses application name as the match criteria</p> <ul style="list-style-type: none"> <li>• &lt;APPLICATION-NAME&gt; – Specify the application name. Each packet's application is matched with the application name specified here. In case of a match, the system forwards the packet.</li> </ul> <p><b>Note:</b> The WiNG system provides approximately 381 canned applications. In addition to these, the database also includes custom-made applications. These are application definitions created using the <a href="#">application</a> command.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <p>schedule &lt;SCHEDULE-POLICY-NAME&gt;</p> | <p>Schedules an enforcement time for this allow rule by associating a schedule policy with it. Use this parameter to apply rule-specific enforcement time.</p> <ul style="list-style-type: none"> <li>• schedule &lt;SCHEDULE-POLICY-NAME&gt; – Associates a schedule policy with the rule. When associated, the rule is enforced only on the days and time configured in the schedule policy. Without the association of a schedule policy, all rules within an application policy are enforced concurrently (defined by the application-policy &gt; enforcement-time command). If scheduling a rule, ensure that the time configured in the schedule policy is a subset of the application policy's enforcement time. In other words the application policy should be active when the rule is being enforced. For example, if the application policy is enforced on Mondays from 10:00 to 22:00 hours and the schedule policy time-rule is set for Fridays, then this rule will never be hit. When enforcing rules at different times the best practice would be to keep the application policy active at all time (i.e., retain the default enforcement-time setting as 'all').</li> <li>• &lt;SCHEDULE-POLICY-NAME&gt; – Specify the policy name (should be existing and configured). After applying a schedule policy, specify a precedence for the rule.</li> </ul> <p><b>Note:</b> In case of no schedule policy being applied, the rule is enforced as per the enforcement-time configured in the application policy. For more information, see <a href="#">enforcement-time</a>.</p> |
| <p>precedence &lt;1-256&gt;</p>              | <p>Assigns a precedence value for this allow rule. The precedence value differentiates between rules applicable to applications and the application categories to which they belong. The allow, deny, mark, rate-limit options are mutually exclusive. In other words, in an application policy, for a specific application or application category, you can create either an allow rule, or a deny rule, or a mark and rate-limit rule.</p> <p>Let us consider application <i>youtube</i> belonging to app-category <i>streaming</i>. The action required is: Allow youtube packets, and deny all other applications belonging to app-category streaming.</p> <p>The rules can be defined as:</p> <pre>#allow application youtube precedence 1 #deny app-category streaming precedence 2</pre> <p>The following configuration is incorrect:</p> <pre>#deny app-category streaming precedence 1 #allow application youtube precedence 2</pre> <p>Once the deny app-category streaming precedence 1 rule is hit, all streaming packets, including youtube, are dropped. Consequently, there are no packets left to apply the subsequent allow rule.</p> <p>The mark and rate-limit rules are the only two actions that can be combined for a specific application or application category type.</p>                                                                                                                                                                                                                                                                                            |

## Examples

The following example shows how to view all built-in, system provided applications:

```
nx9500-6C8809(config-app-policy-test)#allow application [TAB]
Display all 300 possibilities? (y or n)
1-clickshare-com 1-upload-com
1-upload-to 10upload-com
123upload-pl 139pan-com
163pan-com 1clickshare-net
1fichier-com 1kxun
2channel 2gis
2shared-com 360mobile
4fastfile-com 4share-ws
Dota\ 2 EA\ Origin
--More--
nx9500-6C8809(config-app-policy-test)#
```

The following examples show two allow rules, allowing access to all packets belonging to the application category 'business' and the application 'Bing':

```
nx9500-6C8809(config-app-policy-Bing)#allow application Bi [TAB]
Bing BitTorrent BitTorrent_encrypted
BitTorrent_plain BitTorrent_uTP BitTorrent_uTP_encrypted
nx9500-6C8809(config-app-policy-Bing)#
```

Note: Bing is not one of the WING built-in database applications. It is a customized application created using the application command.

```
nx9500-6C8809(config-app-policy-Bing)#allow application Bing precedence 1
nx9500-6C8809(config-app-policy-Bing)#allow app-category [TAB]
all antivirus\ update audio
business conference custom
database filetransfer gaming
generic im mail
mobile network\ management other
p2p remote_control social\ networking
standard streaming tunnel
video voip web
nx9500-6C8809(config-app-policy-Bing)#
nx9500-6C8809(config-app-policy-Bing)#allow app-category business precedence 2
nx9500-6C8809(config-app-policy-Bing)#show context
application-policy Bing
 allow application Bing precedence 1
 allow app-category business precedence 2
nx9500-6C8809(config-app-policy-Bing)#
```

The following example shows an application policy 'SocialNet' having an allow rule with an associated schedule policy named 'FaceBook':

```
nx9500-6C8809(config-app-policy-SocialNet)#allow application facebook schedule Facebook
precedence 1
nx9500-6C8809(config-app-policy-SocialNet)#show context
application-policy SocialNet
 description "This application policy relates to Social Networking sites."
 allow application facebook schedule FaceBook precedence 1
nx9500-6C8809(config-app-policy-SocialNet)#
```

The schedule policy 'FaceBook' configuration is as follows. As per this policy, the above allow rule will apply to all FaceBook packets every Friday between 13:00 and 18:00 hours.

```
nx9500-6C8809(config-schedule-policy-FaceBook)#show context
schedule-policy FaceBook
 description "Allows FaceBook traffic on Fridays."
 time-rule days friday start-time 13:00 end-time 18:00
nx9500-6C8809(config-schedule-policy-FaceBook)#
```

## Related Commands

|                                                              |                                                     |
|--------------------------------------------------------------|-----------------------------------------------------|
| <code>no (application-policy-config-mode)</code> on page 282 | Removes this allow rule from the application policy |
|--------------------------------------------------------------|-----------------------------------------------------|

### deny (application-policy-config-mode)

Creates a deny rule and configures the match criteria based on which packets are filtered and the deny access action applied

Supported in the following platforms:

- Access Points — AP 7522, AP 7532
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
deny [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>] schedule <SCHEDULE-POLICY-NAME> (precedence <1-256>)
```

#### Parameters

```
deny [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>] schedule <SCHEDULE-POLICY-NAME> (precedence <1-256>)
```

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| deny                                   | Creates a deny rule and configures the match criteria. The options are app-category and application.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| app-category [<APP-CATEGORY-NAME> all] | Uses application category as the match criteria <ul style="list-style-type: none"><li>• &lt;APP-CATEGORY-NAME&gt; - Specify the application category name. The options are: antivirus\ update, audio, business, conference, custom, database, file transfer, gaming, generic, im, mail, mobile, network\ management, other, p2p, remote_control, social\ networking, standard, streaming, tunnel, video, voip, and web. Each packet's app-category is matched with the value specified here. In case of a match, the system drops the packet.</li><li>• all - The system drops all packets irrespective of the application category.</li></ul> |
| application <APPLICATION-NAME>         | Uses application name as the match criteria <ul style="list-style-type: none"><li>• &lt;APPLICATION-NAME&gt; - Specify the application name. Each packet's application is matched with the application name specified here. In case of a match, the system drops the packet.</li></ul> <p>There are approximately 300 canned applications in the database. In addition to these, the database displays custom-made applications also. These are application definitions created using the application command.</p>                                                                                                                             |

|                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>schedule &lt;SCHEDULE-POLICY-NAME&gt;</p> | <p>Schedules an enforcement time for this deny rule by associating a schedule policy with it. Use this parameter to apply rule-specific enforcement time.</p> <ul style="list-style-type: none"> <li>• schedule &lt;SCHEDULE-POLICY-NAME&gt; - Associates a schedule policy with the rule. When associated, the rule is enforced only on the days and time configured in the schedule policy. Without the association of a schedule policy, all rules within an application policy are enforced concurrently (defined by the application-policy &gt; enforcement-time command). If scheduling a rule, ensure that the time configured in the schedule policy is a subset of the application policy's enforcement time. In other words the application policy should be active when the rule is being enforced. For example, if the application policy is enforced on Mondays from 10:00 to 22:00 hours and the schedule policy time-rule is set for Fridays, then this rule will never be hit. When enforcing rules at different times the best practice would be to keep the application policy active at all time (i.e., retain the default enforcement-time setting as 'all').</li> <li>• &lt;SCHEDULE-POLICY-NAME&gt; - Specify the policy name (should be existing and configured). After applying a schedule policy, specify a precedence for the rule.</li> </ul> <p>In case of no schedule policy being applied, the rule is enforced as per the enforcement-time configured in the application policy. For more information, see <a href="#">enforcement-time</a>.</p> |
| <p>precedence &lt;1-256&gt;</p>              | <p>Assigns a precedence value for this deny rule. The precedence value differentiates between rules applicable to applications and the application categories to which they belong. The allow, deny, mark, rate-limit options are mutually exclusive. In other words, in an application policy, for a specific application or application category, you can create either an allow rule, or a deny rule, or a mark and rate-limit rule. Let us consider application <i>youtube</i> belonging to app-category <i>streaming</i>. The rules can be defined as:</p> <pre>#allow application youtube precedence 1 #deny app-category streaming precedence 2</pre> <p>The following configuration is incorrect:</p> <pre>#deny app-category streaming precedence 1 #allow application youtube precedence 2</pre> <p>Once the deny app-category streaming precedence 1 rule is hit, all streaming packets, including youtube, are dropped. Consequently, there are no packets left to apply the subsequent allow rule.</p> <p>The mark and rate-limit rules are the only two actions that can be combined for a specific application or application category type.</p>                                                                                                                                                                                                                                                                                                                                                                                                                 |

## Examples

The following example shows one deny rule, denying access to all packets belonging to the application category 'social\ networking':

```
nx9500-6C8809(config-app-policy-Bing)#deny app-category social\ networking precedence 3
nx9500-6C8809(config-app-policy-Bing)#show context
application-policy Bing
 allow application Bing precedence 1
 allow app-category business precedence 2
 deny app-category "social networking" precedence 3
nx9500-6C8809(config-app-policy-Bing)#
```

The following example displays the schedule policy 'DenyS-N' settings. The time-rule defined in the policy is all weekdays from 9:30 AM to 11:30 PM.

```
nx9500-6C8809(config-schedule-policy-DenyS-N)#show context
schedule-policy DenyS-N
 description "Denies all social Networking sites on weekdays."
 time-rule days weekdays start-time 09:30 end-time 23:30
nx9500-6C8809(config-schedule-policy-DenyS-N)#
```

The following example displays the schedule policy 'FaceBook' settings. The time-rule defined in the policy is Friday from 1:00 PM to 6:00 PM.

```
nx9500-6C8809(config-schedule-policy-FaceBook)#show context
schedule-policy FaceBook
 description "Allows FaceBook traffic on Fridays."
 time-rule days friday start-time 13:00 end-time 18:00
nx9500-6C8809(config-schedule-policy-FaceBook)#
```

The following example shows an application policy 'SocialNet' defining an allow and deny rule. Both rules have different enforcement time, defined by their respective schedule policies (DenyS-N and FaceBook). As per these two schedule policy settings, this application policy:

- Denies all social\ networking sites on weekdays (barring Fridays between 1:00 PM to 6:00 PM) from 9:30 AM to 11:30 PM.
- On Fridays, between 1:00 PM to 6:00 PM, it:
  - Denies all social\ networking sites except Facebook.

```
nx9500-6C8809(config-app-policy-SocialNet)#show context
application-policy SocialNet
 description "This application policy relates to Social Networking sites."
 allow application facebook schedule FaceBook precedence 1
 deny app-category "social networking" schedule DenyS-N precedence 2
nx9500-6C8809(config-app-policy-SocialNet)#
```

#### Related Commands

|                                                              |                                                    |
|--------------------------------------------------------------|----------------------------------------------------|
| <code>no (application-policy-config-mode)</code> on page 282 | Removes this deny rule from the application policy |
|--------------------------------------------------------------|----------------------------------------------------|

`description (application-policy-config-mode)`

Configures a brief description for this application policy that enables you to differentiate it from other application policies

Supported in the following platforms:

- Access Points — AP 7522, AP 7532
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
description <LINE>
```

#### Parameters

```
description <LINE>
```

|                                       |                                                                                                                                                                                      |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>description &lt;LINE&gt;</code> | Configures this application policy's description <ul style="list-style-type: none"><li>• &lt;LINE&gt; - Specify a brief description not exceeding 80 characters in length.</li></ul> |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config-app-policy-Bing)#description "This application policy allows Bing
search engine packets"
nx9500-6C8809(config-app-policy-Bing)#show context
application-policy Bing
 description "This application policy allows Bing search engine packets"
 allow application Bing precedence 1
 allow app-category business precedence 2
 deny app-category "social networking" precedence 3
nx9500-6C8809(config-app-policy-Bing)#
```

## Related Commands

`no (application-policy-config-mode)` Removes this application policy's description  
on page 282

### enforcement-time (application-policy-config-mode)

Configures an enforcement time period in days and hours for this application policy. The enforcement time is applicable only to those rules, within the application policy, that do not have a schedule policy associated. By default an application policy is enforced on all days.

#### Note



Schedule policies are a means of enforcing allow/deny/mark/rate-limit rules at different time periods. If no schedule policy is applied, all rules within an application policy are enforced at the time specified using this enforcement-time command. For more information on configuring a schedule policy, see [schedule-policy](#).

Supported in the following platforms:

- Access Points — AP 7522, AP 7532
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
enforcement-time days [sunday|monday|tuesday|wednesday|thursday|friday|saturday|all|weekends|weekdays] {start-time <HH:MM> end-time <HH:MM>}
```

#### Parameters

```
enforcement-time days [sunday|monday|tuesday|wednesday|thursday|friday|saturday|all|weekends|weekdays] {start-time <HH:MM> end-time <HH:MM>}
```

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| enforcement-time days               | <p>Enforces this application policy on only on the days specified here</p> <ul style="list-style-type: none"><li>• sunday – Enforces the policy only on Sundays</li><li>• monday – Enforces the policy only on Mondays</li><li>• tuesday – Enforces the policy only on Tuesdays</li><li>• wednesday – Enforces the policy only on Wednesdays</li><li>• thursday – Enforces the policy only on Thursdays</li><li>• friday – Enforces the policy only on Fridays</li><li>• saturday – Enforces the policy only on Saturdays</li><li>• all – Enforces the policy on all days. This is the default setting.</li><li>• weekends – Enforces the policy only on weekends</li><li>• weekdays – Enforces the policy only on weekdays</li></ul> <p>In case no enforcement time is specified, the application policy is enforced on all days (i.e., always active).<br/>If using schedule policies with the allow/deny/mark/rate-limit rules, the best practice would be to keep the application policy active at all time (i.e., retain the default enforcement-time setting of 'all').</p> |
| start-time <HH:MM> end-time <HH:MM> | <p>Optional. Configures this application policy's enforcement period</p> <ul style="list-style-type: none"><li>• start-time – Configures the start time. This is the time at which the application policy enforcement begins.</li><li>• end-time – Configures the end time. This is the time at which the application policy enforcement ends.<ul style="list-style-type: none"><li>• &lt;HH:MM&gt; – Specify the start and end time in the HH:MM format.</li></ul></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## Examples

```
nx9500-6C8809(config-app-policy-Bing)#enforcement-time days weekdays start-time 10:30 end-time 20:00
nx9500-6C8809(config-app-policy-Bing)#show context
application-policy Bing
description "This application policy allows Bing search engine packets"
enforcement-time days weekdays start-time 10:30 end-time 20:00
allow application Bing precedence 1
allow app-category business precedence 2
deny app-category "social networking" precedence 3
nx9500-6C8809(config-app-policy-Bing)#
```

## Related Commands

|                                                  |                                                                  |
|--------------------------------------------------|------------------------------------------------------------------|
| <code>no (application-policy-config-mode)</code> | Removes this application policy's enforcement period on page 282 |
|--------------------------------------------------|------------------------------------------------------------------|

## logging (application-policy-config-mode)

Enables DPI application recognition logging. It also sets the logging level.

DPI is an advanced packet analysis technique, which analyzes packet and packet content headers to determine the nature of network traffic. When enabled, DPI inspects packets of all flows to identify applications (such as, Netflix, Twitter, Facebook, etc.) and extract metadata (such as, host name, server name, TCP-RTT, etc.) for further use by the WiNG firewall.

Supported in the following platforms:

- Access Points — AP 7522, AP 7532
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

## Syntax

```
logging [level|on]
logging on
logging level [<0-7>|alerts|critical|debugging|emergencies|errors|informational|
notifications|warnings]
```

## Parameters

```
logging on
```

|                         |                                                                                                             |
|-------------------------|-------------------------------------------------------------------------------------------------------------|
| <code>logging on</code> | Enables logging of application recognition hits made by the DPI engine. This option is disabled by default. |
|-------------------------|-------------------------------------------------------------------------------------------------------------|

```
logging level [<0-7>|alerts|critical|debugging|emergencies|errors|informational|
notifications|warnings]
```



```
logging level [<0-7>|alerts| critical|
debugging| emergencies|errors|
informational| notifications| warnings]
```

Sets the logging level for application recognition hits made by the DPI engine. This option is disabled by default.

- <0-7> - Sets the message logging severity level on a scale of 0 - 7
- emergencies - Severity level 0: System is unusable
- alerts - Severity level 1: Requires immediate action
- critical - Severity level 2: Critical conditions
- errors - Severity level 3: Error conditions
- warnings - Severity level 4: Warning conditions
- notifications - Severity level 5: Normal but significant conditions (this is the default setting)
- informational - Severity level 6: Informational messages
- debugging - Severity level 7: Debugging messages

### Examples

```
nx9500-6C8809(config-app-policy-Bing)#logging level critical
nx9500-6C8809(config-app-policy-Bing)#show context
application-policy Bing
 description "This application policy allows Bing search engine packets"
 enforcement-time days weekdays start-time 12:30 end-time 20:00
 allow application Bing precedence 1
 allow app-category business precedence 2
 deny app-category "social networking" precedence 3
 logging level critical
nx9500-6C8809(config-app-policy-Bing)#
```

### Related Commands

**no (application-policy-config-mode)** on page 282

Resets the logging level to default (notifications). And the no > logging > on command disables DPI logging.

## mark (application-policy-config-mode)

Creates a mark rule and configures the match criteria based on which packets are marked

Marks packets, matching a specified set of application categories or applications/protocols, with 802.1p priority level or DSCP ToS (type of service) code. Marking packets is a means of identifying them for specific actions, and is used to provide different levels of service to different traffic types.

WiNG, nx9500-6C8809

Supported in the following platforms:

- Access Points — AP 7522, AP 7532
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

### Syntax

```
mark [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>] [8021p <0-7>|dscp <0-63>] schedule <SCHEDULE-POLICY-NAME> (precedence <1-256>)
```

### Parameters

```
mark [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>] [8021p <0-7>|dscp <0-63>] schedule <SCHEDULE-POLICY-NAME> (precedence <1-256>)
```

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mark                                   | Creates a mark rule and configures the match criteria. When applied, the rule marks packets, matching the criteria configured here, with 802.1p priority value or DSCP code. The match criteria options are: app-category and application.                                                                                                                                                                                                                                                                                                                                                                                                          |
| app-category [<APP-CATEGORY-NAME> all] | <p>Uses application category as the match criteria</p> <ul style="list-style-type: none"> <li>• &lt;APP-CATEGORY-NAME&gt; – Specify the application category. The options are: antivirus\ update, audio, business, conference, custom, database, file transfer, gaming, generic, im, mail, mobile, network\ management, other, p2p, remote_control, social\ networking, standard, streaming, tunnel, video, voip, and web. Each packet's app-category is matched with the value specified here. In case of a match, the system marks the packet.</li> <li>• all – The system marks all packets irrespective of the application category.</li> </ul> |
| application <APPLICATION-NAME>         | <p>Uses application name as the match criteria</p> <ul style="list-style-type: none"> <li>• &lt;APPLICATION-NAME&gt; – Specify the application name. Each packet's application is matched with the application name specified here. In case of a match, the system marks the packet.</li> </ul> <p>The WiNG database provides approximately 300 canned applications. In addition to these, the database includes custom-made applications. These are application definitions created using the <a href="#">application</a> command.</p>                                                                                                             |
| 8021p <0-7>                            | <p>Marks packets matching the specified criteria with 802.1p priority value</p> <ul style="list-style-type: none"> <li>• &lt;0-7&gt; – Specify a value from 0 - 7.</li> </ul> <p>The IEEE 802.1p signaling standard enables marking of layer 2 network traffic. Layer 2 network devices (such as switches), using 802.1p standards, group traffic into classes based on their 802.1p priority value, which is appended to the packet's MAC header. In case of traffic congestion, packets with higher priority get precedence over lower priority packets and are forwarded first.</p>                                                              |
| dscp <0-63>                            | <p>Marks packets matching the specified criteria with DSCP ToS code</p> <ul style="list-style-type: none"> <li>• &lt;0-63&gt; – Specify a value from 0 - 63.</li> </ul> <p>The DSCP protocol marks layer 3 network traffic. Layer 3 network devices (such as routers) using DSCP, mark each layer 3 packet with a six-bit DSCP code, which is appended to the packet's IP header. Each DSCP code is assigned a corresponding level of service, enabling packet prioritization.</p>                                                                                                                                                                  |

|                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>schedule &lt;SCHEDULE-POLICY-NAME&gt;</p> | <p>Schedules an enforcement time for this mark rule by associating a schedule policy with it. Use this parameter to apply rule-specific enforcement time.</p> <ul style="list-style-type: none"> <li>• schedule &lt;SCHEDULE-POLICY-NAME&gt; – Associates a schedule policy with the rule. When associated, the rule is enforced only on the days and time configured in the schedule policy. Without the association of a schedule policy, all rules within an application policy are enforced concurrently (defined by the application-policy &gt; enforcement-time command). If scheduling a rule, ensure that the time configured in the schedule policy is a subset of the application policy's enforcement time. In other words the application policy should be active when the rule is being enforced. For example, if the application policy is enforced on Mondays from 10:00 to 22:00 hours and the schedule policy time-rule is set for Fridays, then this rule will never be hit. When enforcing rules at different times the best practice would be to keep the application policy active at all time (i.e., retain the default enforcement-time setting as 'all').</li> <li>• &lt;SCHEDULE-POLICY-NAME&gt; – Specify the policy name (should be existing and configured). After applying a schedule policy, specify a precedence for the rule.</li> </ul> <p>In case of no schedule policy being applied, the rule is enforced as per the enforcement-time configured in the application policy. For more information, see <a href="#">enforcement-time</a>.</p> |
| <p>precedence &lt;1-256&gt;</p>              | <p>Assigns a precedence value for this mark rule. The precedence value differentiates between rules applicable to applications and the application categories they belong. The allow, deny, mark, rate-limit options are mutually exclusive. In other words, in an application policy, for a specific application or application category, you can create either an allow rule, or a deny rule, or a mark and rate-limit rule. Let us consider application <i>youtube</i> belonging to app-category <i>streaming</i>. The action required is: Allow youtube packets and deny all other applications belonging to app-category streaming. The rules can be defined as:</p> <pre>#allow application youtube precedence 1 #deny app-category streaming precedence 2</pre> <p>The following configuration is incorrect:</p> <pre>#deny app-category streaming precedence 1 #allow application youtube precedence 2</pre> <p>Once the deny app-category streaming precedence 1 rule is hit, all streaming packets, including youtube, are dropped. Consequently, there are no packets left to apply the subsequent allow rule.</p> <p>The mark and rate-limit rules are the only two actions that can be combined for a specific application or application category type.</p>                                                                                                                                                                                                                                                                                                       |

### Examples

```
nx9500-6C8809(config-app-policy-Bing)#mark app-category video dscp 9 precedence 4
nx9500-6C8809(config-app-policy-Bing)#mark application facetime dscp 10 precedence 5
nx9500-6C8809(config-app-policy-Bing)#show context
application-policy Bing
description "This application policy allows Bing search engine packets"
enforcement-time days weekdays start-time 12:30 end-time 20:00
allow application Bing precedence 1
allow app-category business precedence 2
deny app-category "social networking" precedence 3
mark app-category video dscp 9 precedence 4
mark application facetime dscp 10 precedence 5
logging level critical
nx9500-6C8809(config-app-policy-Bing)#
```

### Related Commands

`no (application-policy-config-mode)` Removes this mark rule from the application policy on page 282

## rate-limit (application-policy-config-mode)

Creates a rate-limit rule and configures the match criteria

Supported in the following platforms:

- Access Points — AP 7522, AP 7532
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

### Syntax

```
rate-limit [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>]
([egress|ingress]) rate <50-1000000> max-burst-size <2-1024> schedule <SCHEDULE-POLICY-NAME> (precedence <1-256>)
```

### Parameters

```
rate-limit [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>]
([egress|ingress]) rate <50-1000000> max-burst-size <2-1024> schedule <SCHEDULE-POLICY-NAME> (precedence <1-256>)
```

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| rate-limit                             | Creates a rate-limit rule and configures the match criteria. When applied, the rule applies a rate-limit to packets that match the criteria configured here. These packets could be incoming, outgoing, or both. The match criteria options are: <i>app-category</i> and <i>application</i> .                                                                                                                                                                                                                                                                                                                                                          |
| app-category [<APP-CATEGORY-NAME> all] | Uses application category as the match criteria <ul style="list-style-type: none"> <li>• &lt;APP-CATEGORY-NAME&gt; – Specify the application category. The options are: antivirus\update, audio, business, conference, custom, database, file transfer, gaming, generic, im, mail, mobile, network\management, other, p2p, remote_control, social\ networking, standard, streaming, tunnel, video, voip, and web. Each packet's app-category is matched with the value specified here. In case of a match, the system rate-limits the packet.</li> <li>• all – The system rate-limits all packets irrespective of the application category.</li> </ul> |
| application <APPLICATION-NAME>         | Uses application name as the match criteria <ul style="list-style-type: none"> <li>• &lt;APPLICATION-NAME&gt; – Specify the application name. Each packet's application is matched with the application name specified here. In case of a match, the system rate-limits the packet.</li> </ul>                                                                                                                                                                                                                                                                                                                                                         |
| [egress ingress]                       | The egress and ingress parameters are recursive and can be used to rate limit either incoming, outgoing, or both incoming and outgoing traffic. <ul style="list-style-type: none"> <li>• egress – Selects the traffic type as outgoing</li> <li>• ingress – Selects the traffic type as outgoing</li> </ul> After selecting the traffic type (incoming/outgoing) configure the rate and maximum burst size.                                                                                                                                                                                                                                            |
| rate <50-1000000>                      | The following parameters are common to the 'egress' and 'ingress' keywords: <ul style="list-style-type: none"> <li>• rate – Configures the rate limit, in Kbps, for both incoming and outgoing packets <ul style="list-style-type: none"> <li>• &lt;50-1000000&gt; – Specify the rate limit from 50 - 1000000 Kbps.</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                             |

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| max-burst-size                  | <p>The following parameters are common to the 'egress' and 'ingress' keywords:</p> <ul style="list-style-type: none"> <li>max-burst-size – Configures the maximum burst size, in Kbytes, for both incoming and outgoing packets</li> <li>&lt;2-1024&gt; – Specify the maximum burst size from 2 - 1024 Kbytes.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| schedule <SCHEDULE-POLICY-NAME> | <p>Schedules an enforcement time for this rate-limit rule by associating a schedule policy with it. Use this parameter to apply rule-specific enforcement time.</p> <ul style="list-style-type: none"> <li>schedule &lt;SCHEDULE-POLICY-NAME&gt; – Associates a schedule policy with the rule. When associated, the rule is enforced only on the days and time configured in the schedule policy. Without the association of a schedule policy, all rules within an application policy are enforced concurrently (defined by the application-policy &gt; enforcement-time command). If scheduling a rule, ensure that the time configured in the schedule policy is a subset of the application policy's enforcement time. In other words the application policy should be active when the rule is being enforced. For example, if the application policy is enforced on Mondays from 10:00 to 22:00 hours and the schedule policy time-rule is set for Fridays, then this rule will never be hit. When enforcing rules at different times the best practice would be to keep the application policy active at all time (i.e., retain the default enforcement-time setting as 'all').</li> <li>&lt;SCHEDULE-POLICY-NAME&gt; – Specify the policy name (should be existing and configured). After applying a schedule policy, specify a precedence for the rule.</li> </ul> <p>In case of no schedule policy being applied, the rule is enforced as per the enforcement-time configured in the application policy. For more information, see <a href="#">enforcement-time</a>.</p> |
| precedence <1-256>              | <p>Assigns a precedence value for this mark rule. The precedence value differentiates between rules applicable to applications and the application categories they belong. The allow, deny, mark, rate-limit options are mutually exclusive. In other words, in an application policy, for a specific application or application category, you can create either an allow rule, or a deny rule, or a mark and rate-limit rule.</p> <p>Let us consider application <i>youtube</i> belonging to app-category <i>streaming</i>. The action required is: Allow youtube packets and deny all other applications belonging to app-category streaming.</p> <p>The rules can be defined as:</p> <pre>#allow application youtube precedence 1 #deny app-category streaming precedence 2</pre> <p>The following configuration is incorrect:</p> <pre>#deny app-category streaming precedence 1 #allow application youtube precedence 2</pre> <p>Once the deny app-category streaming precedence 1 rule is hit, all streaming packets, including youtube, are dropped. Consequently, there are no packets left to apply the subsequent allow rule.</p> <p>The mark and rate-limit rules are the only two actions that can be combined for a specific application or application category type.</p>                                                                                                                                                                                                                                                                                           |

### Examples

```
nx9500-6C8809(config-app-policy-Bing)#rate-limit application BGP ingress rate 100
max-burst-size 25 egress rate 50 max-burst-size 25 precedence 6
nx9500-6C8809(config-app-policy-Bing)#show context
application-policy Bing
description "This application policy allows Bing search engine packets"
enforcement-time days weekdays start-time 12:30 end-time 20:00
allow application Bing precedence 1
allow app-category business precedence 2
deny app-category "social networking" precedence 3
```

```

mark app-category video dscp 9 precedence 4
mark application facetime dscp 10 precedence 5
rate-limit application BGP ingress rate 100 max-burst-size 25 egress rate 50 max-burst-
size 25 precedence 6
logging level critical
nx9500-6C8809(config-app-policy-Bing)#

```

#### Related Commands

|                                                  |                                                                      |
|--------------------------------------------------|----------------------------------------------------------------------|
| <code>no (application-policy-config-mode)</code> | Removes this rate-limit rule from the application policy on page 282 |
|--------------------------------------------------|----------------------------------------------------------------------|

#### no (application-policy-config-mode)

Removes or resets this application policy's settings

Supported in the following platforms:

- Access Points — AP 7522, AP 7532
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

#### Syntax

```

no [allow|deny|description|enforcement-time|logging|mark|rate-limit]
no allow [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>]
precedence <1-256>
no deny [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>] precedence
<1-256>
no description
no enforcement-time days [sunday|monday|tuesday|wednesday|thursday|friday|saturday|all|
weekends|weekdays]
no logging [level|on]
no mark [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>] precedence
<1-256>
no rate-limit [app-category [<APP-CATEGORY-NAME>|all]|application <APPLICATION-NAME>]
precedence <0-256>

```

#### Parameters

```
no <PARAMETERS>
```

|                                    |                                                                                   |
|------------------------------------|-----------------------------------------------------------------------------------|
| <code>no &lt;PARAMETERS&gt;</code> | Removes or resets this application policy settings based on the parameters passed |
|------------------------------------|-----------------------------------------------------------------------------------|

#### Examples

The following example shows the application policy 'Bing' settings before the 'no' commands are executed:

```

nx9500-6C8809(config-app-policy-Bing)#show context
application-policy Bing
description "This application policy allows Bing search engine packets"
enforcement-time days weekdays start-time 12:30 end-time 20:00
allow application Bing precedence 1
allow app-category business precedence 2
deny app-category "social networking" precedence 3
mark app-category video dscp 9 precedence 4
mark application facetime dscp 10 precedence 5
rate-limit application BGP ingress rate 100 max-burst-size 25 egress rate 50 max-burst-
size 25 precedence 6

```

```

logging level critical
nx9500-6C8809(config-app-policy-Bing)#
nx9500-6C8809(config-app-policy-Bing)#no allow app-category business precedence 2
nx9500-6C8809(config-app-policy-Bing)#no deny app-category social\ networking precedence 3

```

The following example shows the application policy 'Bing' settings after the 'no' commands are executed:

```

nx9500-6C8809(config-app-policy-Bing)#show context
application-policy Bing
description "This application policy allows Bing search engine packets"
enforcement-time days weekdays start-time 12:30 end-time 20:00
allow application Bing precedence 1
mark app-category video dscp 9 precedence 4
mark application facetime dscp 10 precedence 5
rate-limit application BGP ingress rate 100 max-burst-size 25 egress rate 50 max-burst-size 25 precedence 6
logging level critical
nx9500-6C8809(config-app-policy-Bing)#

```

### *association-acl-policy*

Configures an association ACL policy. This policy defines a list of devices allowed or denied access to the network.

#### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### **Syntax**

```
association-acl-policy <ASSOCIATION-ACL-POLICY-NAME>
```

#### **Parameters**

```
association-acl-policy <ASSOCIATION-ACL-POLICY-NAME>
```

|                               |                                                                                       |
|-------------------------------|---------------------------------------------------------------------------------------|
| <ASSOCIATION-ACL-POLICY-NAME> | Specify the association ACL policy name. If the policy does not exist, it is created. |
|-------------------------------|---------------------------------------------------------------------------------------|

#### **Examples**

```

NOC-NX9500(config)#association-acl-policy test
NOC-NX9500(config-assoc-acl-test)#?
Association ACL Mode commands:
deny Specify MAC addresses to be denied
no Negate a command or set its defaults
permit Specify MAC addresses to be permitted

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

```

```
NOC-NX9500(config-assoc-acl-test)#
```

## Related Commands

|                 |                                     |
|-----------------|-------------------------------------|
| <code>no</code> | Removes this Association ACL Policy |
|-----------------|-------------------------------------|



### Note

For more information on the association-acl-policy, see [ASSOCIATION-ACL-POLICY](#).

## *auto-provisioning-policy*

Configures an auto provisioning policy. This policy configures the automatic provisioning of device adoption. The policy configures how an AP is adopted based on its type.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
auto-provisioning-policy <AUTO-PROVISIONING-POLICY-NAME>
```

### Parameters

```
auto-provisioning-policy <AUTO-PROVISIONING-POLICY-NAME>
```

|                                 |                                                                                         |
|---------------------------------|-----------------------------------------------------------------------------------------|
| <AUTO-PROVISIONING-POLICY-NAME> | Specify the auto provisioning policy name. If the policy does not exist, it is created. |
|---------------------------------|-----------------------------------------------------------------------------------------|

### Examples

```
NOC-NX9500(config)#auto-provisioning-policy test
NOC-NX9500(config-auto-provisioning-policy-test)#?
Auto-Provisioning Policy Mode commands:
 adopt Add rule for device adoption
 auto-create-rfd-template When RF Domain specified by the matching rule
 template does not exist create new RF Domain
 automatically
 default-adoption Adopt devices even when no matching rules are
 found. Assign default profile and default
 rf-domain
 deny Add rule to deny device adoption
 evaluate-always Set the flag to evaluate the policy everytime,
 regardless of previous adoption status
 no Negate a command or set its defaults
 redirect Add rule to redirect device adoption
 upgrade Add rule for device upgrade

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
```



---

|         |                                                   |
|---------|---------------------------------------------------|
| service | Service Commands                                  |
| show    | Show running system information                   |
| write   | Write running configuration to memory or terminal |

NOC-NX9500(config-auto-provisioning-policy-test)#

### Related Commands

|    |                                              |
|----|----------------------------------------------|
| no | Removes an existing Auto Provisioning policy |
|----|----------------------------------------------|



#### Note

For more information on the auto-provisioning-policy, see [AUTO-PROVISIONING-POLICY](#).

## bgp

Configures BGP (Border Gateway Protocol) settings

BGP is an inter-ISP routing protocol which establishes routing between ISPs (Internet Service Providers). ISPs use BGP to exchange routing and reachability information between AS (Autonomous Systems) on the Internet. BGP makes routing decisions based on paths, network policies and/or rules configured by network administrators. The primary role of a BGP system is to exchange network reachability information with other BGP peers. This information includes information on AS that the reachability information traverses. This information is sufficient to create a graph of AS connectivity from which routing decisions can be created and rules enforced.

An AS is a set of routers under the same administration that use IGP (Interior Gateway Protocol) and common metrics to define how to route packets within the AS. AS uses inter-AS routing to route packets to other ASs. For an external AS, an AS appears to have a single coherent interior routing plan and presents a consistent picture of the destinations reachable through it.

Routing information exchanged through BGP supports only destination based forwarding (it assumes a router forwards packets based on the destination address carried in the IP header of the packet).

BGP uses TCP as its transport protocol. This eliminates the need to implement explicit update fragmentation, retransmission, acknowledgment, and sequencing. BGP listens on TCP port 179. The error notification mechanism used in BGP assumes that TCP supports a graceful close (all outstanding data is delivered before the connection is closed).

WiNG, nx9500-6C8809

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
bgp [as-path-list|community-list|extcommunity-list|ip-access-list|ip-prefix-list] <LIST-NAME>
```

## Parameters

bgp [as-path-list|community-list|extcommunity-list|ip-access-list|ip-prefix-list] <LIST-NAME>

|                               |                                                                                                                                                                              |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| as-path-list <LIST-NAME>      | Creates an AS path list and enters its configuration mode <ul style="list-style-type: none"><li>&lt;LIST-NAME&gt; - Provide the AS-PATH-LIST name.</li></ul>                 |
| community-list <LIST-NAME>    | Creates a community list and enters its configuration mode <ul style="list-style-type: none"><li>&lt;LIST-NAME&gt; - Provide the COMMUNITY-LIST name.</li></ul>              |
| extcommunity-list <LIST-NAME> | Creates an extended community list and enters its configuration mode <ul style="list-style-type: none"><li>&lt;LIST-NAME&gt; - Provide the EXTCOMMUNITY-LIST name.</li></ul> |
| ip-access-list <LIST-NAME>    | Creates a BGP IP access list and enters its configuration mode <ul style="list-style-type: none"><li>&lt;LIST-NAME&gt; - Provide the BGP IP-ACCESS-LIST name.</li></ul>      |
| ip-prefix-list <LIST-NAME>    | Creates a BGP IP prefix list and enters its configuration mode <ul style="list-style-type: none"><li>&lt;LIST-NAME&gt; - Provide the BGP IP-PREFIX-LIST name.</li></ul>      |

## Examples

```
nx9500-6C8809(config)#bgp ?
 as-path-list BGP AS path list Configuration
 community-list Add a community list entry
 extcommunity-list Add a extended community list entry (EXPERIMENTAL)
 ip-access-list Add an access list entry
 ip-prefix-list Build a prefix list
```

```
nx9500-6C8809(config)#
nx9500-6C8809(config)#bgp as-path-list AS-TEST-PATH
nx9500-6C8809(config-bgp-as-path-list-AS-TEST-PATH)#?
BGP AS Path List Mode commands:
 deny Specify packets to reject
 no Negate a command or set its defaults
 permit Specify packets to forward

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal
```

```
nx9500-6C8809(config-bgp-as-path-list-AS-TEST-PATH)#
```

## Related Commands

[no \(global-config-mode\)](#) Modifies BGP settings, based on the parameters passed on page 475



### Note

For more information on the association-acl-policy, see [BORDER GATEWAY PROTOCOL](#) on page 1852.

## *bonjour-gw-discovery-policy*

Bonjour is Apple's zero-configuration networking (Zeroconf) implementation. Bonjour enables automatic IP address assignment, name to address resolution, and service discovery without having to configure a DHCP server, DNS server, and Directory server. When configured and applied on a WLAN, the Bonjour Gateway Discovery policy queries for and locates Bonjour devices (printers, computers, file-sharing servers, etc.) and services these computers provide over a local network. Bonjour works only within a single broadcast domain. However, with a special DNS configuration, it can be extended to find services across broadcast domains.

Use this command to configure a Bonjour GW Discovery policy. The policy defines a list of services clients can discover across subnets. A maximum of 8 (eight) policies can be created on access points, wireless controllers, or service platforms.

When configured and applied, this feature enables Bonjour services on local and tunneled VLANs.

### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### **Syntax**

```
bonjour-gw-discovery-policy <POLICY-NAME>
```

### **Parameters**

```
bonjour-gw-discovery-policy <POLICY-NAME>
```

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;POLICY-NAME&gt;</b> | <p>Specify the Bonjour GW Discovery policy name. If the policy does not exist, it is created. In the Bonjour GW Discovery policy configuration mode, use the <code>allow-service</code> keyword to configure the services that the Bonjour gateway is allowed to discover. A maximum of 16 (sixteen) service rules can be created. Optionally, you can restrict this facility for users on specific VLANs. To do so, specify the VLAN IDs.</p> <p>Execute the <code>bonjour-gw-forwarding-policy</code> command to enable forwarding of Bonjour service responses across VLANs.</p> <p>To associate a Bonjour GW Discovery policy with a WLAN, in the WLAN configuration mode, execute the following command: <b>use &gt; <code>bonjour-gw-discovery-policy</code> &gt; <code>&lt;POLICY-NAME&gt;</code></b>. For more information, see <a href="#">use</a> on page 1058.</p> <p>To associate a Bonjour GW Discovery policy with a VLAN, in the interface VLAN configuration mode, execute the following command: <b>use &gt; <code>bonjour-gw-discovery-policy</code> &gt; <code>&lt;POLICY-NAME&gt;</code></b>. For more information, see <a href="#">use</a> on page 1058.</p> <p>To associate a Bonjour GW Discovery policy with a user role, in the <code>role-policy - user-role - configuration</code> mode, execute the following command: <b>use &gt; <code>bonjour-gw-discovery-policy</code> &gt; <code>&lt;POLICY-NAME&gt;</code></b>. For more information, see <a href="#">use</a>.</p> |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### **Examples**

```
nx9500-6C8809(config)#bonjour-gw-discovery-policy TestPolicy
nx9500-6C8809(config-bonjour-gw-discovery-policy-TestPolicy)#?
commands:
 allow-service Allow Bonjour Service on local or tunneled vlan,Optionally
 VLAN IDs can be given so service will be discovered for those
 vlan only
 no Negate a command or set its defaults
```

```

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

```

nx9500-6C8809 (config-bonjour-gw-discovery-policy-TestPolicy)#sIsEtU\_@3691

### Related Commands

|           |                                                 |
|-----------|-------------------------------------------------|
| <b>no</b> | Removes an existing Bonjour GW Discovery policy |
|-----------|-------------------------------------------------|

### bonjour-gw-discovery-policy-config-commands

The following table summarizes the Bonjour Gateway Discovery Policy configuration mode commands:

**Table 10: Bonjour GW Discovery Policy Config Commands**

| Command                                                                            | Description                                                                                                                                            |
|------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">allow-service (bonjour-gw-discovery-policy-cogig-mode)</a> on page 288 | Configures the Bonjour Services that can be discovered on Local or Tunneled VLANs. It configures the local VLANs on which these services can be found. |
| <a href="#">no (bonjour-gw-discovery-policy-config-mode)</a> on page 290           | Removes or modifies the Bonjour Gateway Discovery policy settings                                                                                      |

#### allow-service (bonjour-gw-discovery-policy-cogig-mode)

Enables discovery of Bonjour devices and the services they provide on Local or Tunneled VLANs

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```

allow-service <BONJOUR-SERVICE-NAME> [local|tunneled]
allow-service <BONJOUR-SERVICE-NAME> local {instance-name contains <WORD>} ({service-vlans <WORD>})
allow-service <BONJOUR-SERVICE-NAME> tunneled {instance-name contains <WORD>}

```

#### Parameters

```

allow-service <BONJOUR-SERVICE-NAME> local {instance-name contains <WORD>} ({service-vlans <WORD>})

```

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| allow-service<br><BONJOUR-SERVICE-NAME> | <p>Configures the services that can be discovered by the Bonjour gateway. And also configures the VLANs on which the selected services can be discovered.</p> <ul style="list-style-type: none"> <li>• &lt;BONJOUR-SERVICE-NAME&gt; – You can either select the Bonjour services from a set of system-provided, pre-defined Apple services, or use an existing alias to define a service not available in the predefined list.</li> </ul> <p>The predefined Apple services available are: Afp, AirPlay, AirPort, AirPrint, AirTunes, AppleTimeMachine, Chromecast, Daap, HomeSharing, Printer, and Scanner.</p> <p>Use the &lt;WORD&gt; keyword to define a service not included in the system-provided, pre-defined list. Ensure this device is registered with the Multicast DNS Responder (mDNSResponder).</p>                                                                                                                                                                                                                               |
| local                                   | Select to enable the discovery of the selected Bonjour Services on the local VLAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| instance-name contains<br><WORD>        | <p>Optional. Specifies the selected Bonjour service's instance name. When specified, the Bonjour service discovery queries contain the instance name. of the service to be discovered.</p> <p>This option is useful especially in large distributed, enterprise networks. Use it to create different instances of a Bonjour service for the different organizations or departments (VLANs) within your network. Creating instances allows you to advertise specific service instances for a specific set of VLANs, instead of advertising top-level Bonjour Services to various allocated VLAN(s).</p> <ul style="list-style-type: none"> <li>• contains &lt;WORD&gt; – Specify the instance name. You can either directly specify the string value to be used as a match criteria, or use a string alias (for example, \$BONJOUR-STRING) to identify the string to match. If using a string alias, ensure that it is existing and configured. For information on configuring a string alias, see <a href="#">alias</a> on page 237.</li> </ul> |
| service-vlans <WORD>                    | Optional. Configures a VLAN or a list of VLANs on which the selected service is discoverable. When specified, Bonjour discovery queries are delivered to all clients on the specified VLANs. Applicable only if enabling Bonjour Services discovery on local VLANs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

```
allow-service <BONJOUR-SERVICE-NAME> tunneled {instance-name contains <WORD>}
```

|                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| allow-service <BONJOUR-SERVICE-NAME> | <p>Configures the services that can be discovered by the Bonjour gateway. And also configures the VLANs on which the selected services can be discovered.</p> <ul style="list-style-type: none"> <li>&lt;BONJOUR-SERVICE-NAME&gt; – You can either select the Bonjour Services from a set of system-provided, pre-defined Apple services, or use an existing alias to define a service not available in the predefined list.</li> </ul> <p>The predefined Apple services available are: Afp, AirPlay, AirPort, AirPrint, AirTunes, AppleTimeMachine, Chromecast, Daap, HomeSharing, Printer, and Scanner.</p> <p>Use the &lt;WORD&gt; keyword to define a service not included in the system-provided, predefine list.</p>                                                                                                                            |
| tunneled                             | Select to enable the discovery of the selected Bonjour Services on tunneled VLANs                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| instance-name contains <WORD>        | <p>Optional. Adds a Bonjour Service instance name. If you have a large enterprise network, use this option to create different Bonjour Service instances for the different organizations or departments (VLANs) within your network. Creating instances allows you to advertise specific service instances for a specific set of VLANs, instead of advertising top-level Bonjour Services to various allocated VLAN(s).</p> <ul style="list-style-type: none"> <li>contains &lt;WORD&gt; – Specify the sub-string to match. You can either directly specify the string value to be used as a match criteria, or use a string alias (for example, \$BONJOUR-STRING) to identify the string to match. If using a string alias, ensure that it is existing and configured. For information on configuring aliases, see <a href="#">alias</a>.</li> </ul> |

### Examples

```

nx9500-6C8809(config-bonjour-gw-discovery-policy-test)#allow-service Afp local
nx9500-6C8809(config-bonjour-gw-discovery-policy-test)#allow-service Printer lo
cal instance-name contains $Bonjour_Service service-vlans 1,2
nx9500-6C8809(config-bonjour-gw-discovery-policy-test)#show context
bonjour-gw-discovery-policy test
 allow-service Printer local service-vlans 1-2 instance-name contains $Bonjour_Service
 allow-service Afp local
nx9500-6C8809(config-bonjour-gw-discovery-policy-test)#

```

Following example configures the string alias named \$Bonjour\_Service:

```

nx9500-6C8809(config)#alias string $Bonjour_Service admin
nx9500-6C8809(config)#commit
nx9500-6C8809(config)#show context include-factory | include alias string
alias string $Bonjour_Service admin
nx9500-6C8809(config)#

```

### Related Commands

|                                                                                                                      |
|----------------------------------------------------------------------------------------------------------------------|
| <p><b>no (global-config-mode)</b> Removes or modifies this Bonjour Gateway Discovery Policy settings on page 475</p> |
|----------------------------------------------------------------------------------------------------------------------|

no (bonjour-gw-discovery-policy-config-mode)

Removes or modifies the Bonjour Gateway Discovery policy settings

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000

- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
no allow-service <BONJOUR-SERVICE-NAME> [local|tunneled] {service-vlans <WORD>}
```

#### Parameters

```
no allow-service <BONJOUR-SERVICE-NAME> [local|tunneled] {service-vlans <WORD>}
```

|                 |                                                                                                         |
|-----------------|---------------------------------------------------------------------------------------------------------|
| no <parameters> | Removes allow-service rules in the selected Bonjour GW Discovery policy, based on the parameters passed |
|-----------------|---------------------------------------------------------------------------------------------------------|

#### Examples

The following example shows the Bonjour GW Discovery policy 'test' settings before the 'no' command is executed:

```
nx9500-6C8809(config-bonjour-gw-discovery-policy-test)#show context
bonjour-gw-discovery-policy test
 allow-service Printer local service-vlans 1-2 instance-name contains $Bonjour_Service
 allow-service Afp local
nx9500-6C8809(config-bonjour-gw-discovery-policy-test)#
nx9500-6C8809(config-bonjour-gw-discovery-policy-test1)#no allow-service Afp local
```

The following example shows the Bonjour GW Discovery policy 'test' settings after the 'no' command was executed:

```
nx9500-6C8809(config-bonjour-gw-discovery-policy-test)#show context
bonjour-gw-discovery-policy test
 allow-service Printer local service-vlans 1-2 instance-name contains $Bonjour_Service
nx9500-6C8809(config-bonjour-gw-discovery-policy-test)#
```

#### *bonjour-gw-forwarding-policy*

Configures a Bonjour GW Forwarding policy. When configured and applied on the controller, the policy defines the service VLANs (the VLANs on which Bonjour services are running) and client VLANs where clients are present. All Bonjour responses from service VLANs are forwarded to client VLANs. A maximum of 2 (two) policies can be created on a wireless controller or service platform. And only 1 (one) policy can be created on an access point.

#### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### **Syntax**

```
bonjour-gw-forwarding-policy <POLICY-NAME>
```

#### **Parameters**

```
bonjour-gw-forwarding-policy <POLICY-NAME>
```

<POLICY-NAME> Specify the Bonjour GW Forwarding policy name. If the policy does not exist, it is created. To receive Bonjour service responses from specific VLANs, specify the VLAN IDs. In the Bonjour GW Forwarding policy configuration mode, provide a list of VLAN IDs from which Bonjour responses can be received (format: 10-20, 25, 30-35). And then specify the list of client VLANs that can access Bonjour services.

Execute the `bonjour-gw-discovery-policy` command to define the Bonjour services allowed on local and tunneled VLANs.

To associate a Bonjour GW Forwarding policy with a device or profile, in the profile/device configuration mode, execute the `use > bonjour-gw-forwarding-policy > <POLICY-NAME>` command. For more information, see [use](#) on page 1232.

## Examples

```

nx9500-6C8809(config)#bonjour-gw-forwarding-policy test
nx9500-6C8809(config-bonjour-gw-forwarding-policy-test)#?
(config-bonjour-gw-forwarding-policy) commands:
 forward-bonjour-response Forwards bonjour service response across vlans
 no Negate a command or set its defaults

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-bonjour-gw-forwarding-policy-test)#

```

## Related Commands

`no` Removes an existing Bonjour GW Forwarding policy

### *bonjour-gw-query-forwarding-policy*

Configures a Bonjour GW Query Forwarding policy and enters its configuration mode. When created and applied, this policy enables forwarding of Bonjour queries across VLANs.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
bonjour-gw-query-forwarding-policy <POLICY-NAME>
```

#### Parameters

```
bonjour-gw-query-forwarding-policy <POLICY-NAME>
```



|                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;POLICY-NAME&gt;</code> | <p>Specify the Bonjour GW Query Forwarding policy name. If the policy does not exist, it is created.</p> <p>In the Bonjour GW Query Forwarding policy configuration mode, specify the 'from' and 'to' VLAN(s). The from-vlans option configures the VLAN(s) that are the source of the Bonjour queries. The to-vlans option configures the destination VLAN(s) that can access the Bonjour queries.</p> <p>To associate a Bonjour GW Query Forwarding policy with a device or profile, in the profile/device configuration mode, execute the <b>use &gt; bonjour-gw-query-forwarding-policy &gt; &lt;POLICY-NAME&gt;</b> command. For more information, see <a href="#">use</a> on page 1232.</p> |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```

nx9500-6C8809(config)#bonjour-gw-query-forwarding-policy test
nx9500-6C8809(config-bonjour-gw-query-forwarding-policy-test)#?
(config-bonjour-gw-query-forwarding-policy) commands:
 forward-bonjour-query Forwards bonjour query across vlans
 no Negate a command or set its defaults

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-bonjour-gw-query-forwarding-policy-test)#

```

### Related Commands

|                                      |                                                                    |
|--------------------------------------|--------------------------------------------------------------------|
| <code>no (global-config-mode)</code> | Removes an existing Bonjour GW Query Forwarding policy on page 475 |
|--------------------------------------|--------------------------------------------------------------------|

### *captive-portal*

Configures a captive portal policy and enters its configuration mode. Once created and configured, use the captive portal policy in the WLAN context, and in the device/profile contexts of the access point or controller hosting the captive portal server.

A captive portal provides secure access using a standard Web browser. Captive portals provide authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the wireless network. Once logged into the captive portal, additional Acknowledgment, Agreement, Welcome, No Service, and Fail pages provides you options to customize the screen flow and user appearance.

Captive portals are recommended for providing guests or visitors authenticated access to network resources when 802.1X EAP is not a viable option. Captive portal authentication does not provide end-user data encryption, but it can be used with static WEP, WPA-PSK or WPA2-PSK encryption.

Authentication for captive portal access requests is performed using a username and password pair, authenticated by an integrated RADIUS server. Authentication for private network access is conducted either locally on the requesting wireless client, or centrally at a data center.

Captive portals use a Web provisioning tool to create guest user accounts directly on the controller, service platform, or access point. The connection medium defined for the Web connection is either HTTP or HTTPS. Both HTTP and HTTPS use a request and response procedure to disseminate information to and from requesting wireless clients.

**Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

**Syntax**

`captive-portal <CAPTIVE-PORTAL-NAME>`

**Parameters**

`captive-portal <CAPTIVE-PORTAL-NAME>`

|                       |                                                                                                             |
|-----------------------|-------------------------------------------------------------------------------------------------------------|
| <CAPTIVE-PORTAL-NAME> | Specify the captive portal name. If a captive portal with the specified name does not exist, it is created. |
|-----------------------|-------------------------------------------------------------------------------------------------------------|

**Examples**

```
nx9500-6C8809(config)#captive-portal test
nx9500-6C8809(config-captive-portal-test)#?
```

Captive Portal Mode commands:

|                                         |                                                                                                                                     |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <code>access-time</code>                | Allowed access time for the client. Used when there is no session time in radius response                                           |
| <code>access-type</code>                | Access type of this captive portal                                                                                                  |
| <code>accounting</code>                 | Configure how accounting records are created for this captive portal policy                                                         |
| <code>bypass</code>                     | Bypass captive portal                                                                                                               |
| <code>connection-mode</code>            | Connection mode for this captive portal                                                                                             |
| <code>custom-auth</code>                | Custom user information                                                                                                             |
| <code>data-limit</code>                 | Enforce data limit for clients                                                                                                      |
| <code>frictionless-onboarding</code>    | Register the client MAC address at ExtremeGuest on redirection                                                                      |
| <code>inactivity-timeout</code>         | Inactivity timeout in seconds. If a frame is not received from client for this amount of time, then current session will be removed |
| <code>ipv6</code>                       | Internet Protocol version 6 (IPv6)                                                                                                  |
| <code>localization</code>               | Configure the FQDN address to get the localization parameters for the client                                                        |
| <code>logout-fqdn</code>                | Configure the FQDN address to logout the session from client                                                                        |
| <code>no</code>                         | Negate a command or set its defaults                                                                                                |
| <code>oauth</code>                      | OAuth 2.0 authentication configuration                                                                                              |
| <code>php-helper</code>                 | Configure the captive portal to use a server for help with php                                                                      |
| <code>post-authentication-vlan</code>   | Configure post authentication vlan for captive portal users                                                                         |
| <code>radius-vlan-assignment</code>     | Enable radius vlan assignment for captive portal users                                                                              |
| <code>redirection</code>                | Configure connection redirection parameters                                                                                         |
| <code>report-loyalty-application</code> | Report customer loyalty application presence in clients                                                                             |
| <code>server</code>                     | Configure captive portal server parameters                                                                                          |
| <code>simultaneous-users</code>         | Particular username can only be used by a certain number of MAC addresses at a time                                                 |

```

terms-agreement User needs to agree for terms and conditions
use Set setting to use
webpage Configure captive portal webpage parameters
webpage-auto-upload Enable automatic upload of internal and advanced
 webpages
webpage-location The location of the webpages to be used for
 authentication. These pages can either be hosted
 on the system or on an external web server.
welcome-back Welcome back page settings

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or
 terminal
nx9500-6C8809(config-captive-portal-test)#

```

### Related Commands

|                 |                                    |
|-----------------|------------------------------------|
| <code>no</code> | Removes an existing captive portal |
|-----------------|------------------------------------|

### captive-portal-mode-commands

The following table summarizes captive portal configuration mode commands:

**Table 11: Captive-Portal-Mode Commands**

| Command                                          | Description                                                                                                                                                     |
|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>access-time</code>                         | Defines a client's access time. It is used when no session time is defined in the RADIUS response.                                                              |
| <code>access-type</code>                         | Configures a captive portal's access type                                                                                                                       |
| <code>accounting</code>                          | Enables a captive portal's accounting records                                                                                                                   |
| <code>bypass</code>                              | Enables bypassing of captive portal detection requests                                                                                                          |
| <code>connection-mode</code>                     | Configures a captive portal's connection mode                                                                                                                   |
| <code>custom-auth</code>                         | Configures custom user information                                                                                                                              |
| <code>data-limit</code>                          | Enforces data limit on captive portal clients                                                                                                                   |
| <code>frictionless-onboarding</code> on page 301 | Enables wireless clients, associated with guest WLANs, to self-register with the ExtremeGuest server.                                                           |
| <code>inactivity-timeout</code>                  | Defines an inactivity timeout in seconds                                                                                                                        |
| <code>ipv6</code> on page 304                    | Configures the IPv6 address of the internal captive portal server                                                                                               |
| <code>localization</code> on page 305            | Configures an FQDN address string that enables the client to receive localization parameters. This command also allows the configuration of a response message. |
| <code>logout-fqdn</code>                         | Clears the logout FQDN address                                                                                                                                  |

**Table 11: Captive-Portal-Mode Commands (continued)**

| Command                                             | Description                                                                                                                                                                             |
|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>no</code>                                     | Reverts the selected captive portal's settings or resets settings to default                                                                                                            |
| <code>oauth</code> on page 307                      | Enables OAuth-based authentication support on the captive portal. When enabled, OAuth allows captive-portal users to sign in to guest WLANs using their Facebook or Google credentials. |
| <code>php-helper</code> on page 308                 | Configures a PHP helper to serve the captive portal's PHP splash pages to guest users using social-media to login to the captive portal.                                                |
| <code>post-authentication-vlan</code>               | Assigns a post authentication RADIUS VLAN for this captive portal's users                                                                                                               |
| <code>radius-vlan-assignment</code>                 | Assigns a RADIUS VLAN for this captive portal                                                                                                                                           |
| <code>redirection</code>                            | Enables redirection of client connections to specified destination ports                                                                                                                |
| <code>report-royalty-application</code> on page 312 | Enables detection of captive portal client's loyalty application presence and stores this information in the captive portal's user database                                             |
| <code>server</code>                                 | Configures the captive portal server settings                                                                                                                                           |
| <code>simultaneous-users</code>                     | Specifies a username used by a MAC address pool                                                                                                                                         |
| <code>terms-agreement</code>                        | Enforces the user to agree to terms and conditions (included in login page) for captive portal access                                                                                   |
| <code>use</code>                                    | Associates a AAA policy and a DNS whitelist with a captive portal                                                                                                                       |
| <code>webpage</code>                                | Configures captive portal Web page settings                                                                                                                                             |
| <code>webpage-auto-upload</code>                    | Enables automatic upload of advanced Web pages on a captive portal                                                                                                                      |
| <code>webpage-location</code>                       | Specifies the location of Web pages used for captive portal authentication                                                                                                              |
| <code>welcome-back</code> on page 326               | Enables the provision of direct Internet access to once-registered, captive-portal guest users on subsequent log-ins                                                                    |

#### access-time

Defines the permitted access time for a client. It is used when no session time is defined in the RADIUS response.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
access-time <10-10080>
```

#### Parameters

```
access-time <10-10080>
```

|                                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------|
| <p>&lt;30-10080&gt; Defines the access time allowed for a wireless client from 10 - 10080 minutes. The default is 1440 minutes.</p> |
|-------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-captive-portal-test)#access-time 35
nx9500-6C8809(config-captive-portal-test)#show context
captive-portal test
 access-time 35
nx9500-6C8809(config-captive-portal-test)#
```

## Related Commands

|    |                                                             |
|----|-------------------------------------------------------------|
| no | Reverts to the default permitted access time (1440 minutes) |
|----|-------------------------------------------------------------|

## access-type

Defines the captive portal's access type. The authentication scheme configured here is applied to wireless clients requesting captive portal guest access to the WiNG network.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
access-type [custom-auth-radius | logging | no-auth | radius | registration]
```

## Parameters

```
access-type [custom-auth-radius | logging | no-auth | radius | registration]
```

|                    |                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| custom-auth-radius | Specifies the custom user information used for authentication (RADIUS lookup of given information, such as name, e-mail address, telephone, etc.). When configured, accessing clients are required to provide a 1-32 character lookup data string used to authenticate their credentials.<br>When selecting this option, use the custom-auth command to configure the required user information.             |
| logging            | Enables logging of user access details.                                                                                                                                                                                                                                                                                                                                                                      |
| no-auth            | Defines no authentication required for a guest. Requesting clients are redirected to the captive portal Welcome page without authentication.                                                                                                                                                                                                                                                                 |
| radius             | Enables RADIUS authentication for wireless clients. A requesting client's user credentials require authentication before access to the captive portal is permitted. This is the default setting.                                                                                                                                                                                                             |
| registration       | Enables captive portal's clients to self register. When enabled, a requesting client's user credentials require authentication locally or through social media credential exchange and validation.<br>If enabled, use the <b>webpage &gt; internal &gt; registration &gt; field</b> command to customize the registration page. If not customized, the default, built-in registration Web page is displayed. |

## Examples

```
nx9500-6C8809(config-captive-portal-test)#access-type logging
nx9500-6C8809(config-captive-portal-test)#show context
captive-portal test
 access-type logging
 access-time 35
nx9500-6C8809(config-captive-portal-test)#
```

## Related Commands

**no** Removes the captive portal access type or reverts to default (radius)

## accounting

Enables support for accounting messages for this captive portal

When enabled, accounting for clients entering and exiting the captive portal is initiated. Accounting is the method of collecting and sending security server information for billing, auditing, and reporting user data. This data includes information, such as start and stop times, executed commands (such as PPP), number of packets and number of bytes transmitted etc. Accounting enables tracking of captive portal services consumed by clients.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
accounting [radius|syslog]
accounting radius
accounting syslog host <IP/HOSTNAME> {port <1-65535>} {proxy-mode [none|through-controller|through-rf-domain-manager]}
```

### Parameters

accounting radius

**radius** Enables support for RADIUS accounting messages. When enabled, this option uses an external RADIUS resource for AAA accounting. This option is disabled by default.

```
accounting syslog host <IP/HOSTNAME> {port <1-65535>} {proxy-mode [none|through-controller|through-rf-domain-manager]}
```

|                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| syslog host <IP/HOSTNAME>                                      | Enables support for syslog accounting messages. When enabled, data relating to wireless client usage of remote access services is logged on the specified external syslog resource. This information assists in differentiating between local and remote users. Remote user information can be archived to an external location for periodic network and user administration. This option is disabled by default. <ul style="list-style-type: none"><li>• host &lt;IP/HOSTNAME&gt; - Specifies the destination where accounting messages are sent. Specify the destination's IP address or hostname.</li></ul> |
| port <1-65535>                                                 | Optional. Specifies the syslog server's listener port <ul style="list-style-type: none"><li>• &lt;1-65535&gt; - Specify the UDP port from 1- 65535. The default is 514.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                              |
| proxy-mode [none through-controller through-rf-domain-manager] | Optional. Specifies the mode of proxying the syslog server <ul style="list-style-type: none"><li>• none - Accounting messages are sent directly to the syslog server</li><li>• through-controller - Accounting messages are sent through the controller configuring the device</li><li>• through-rf-domain-manager - Accounting messages are sent through the local RF Domain manager</li></ul>                                                                                                                                                                                                                |

### Examples

```
nx9500-6C8809(config-captive-portal-test)#accounting syslog host 172.16.10.13 port 1
nx9500-6C8809(config-captive-portal-test)#show context
captive-portal test
```

```
access-type logging
access-time 35
accounting syslog host 172.16.10.13 port 1
nx9500-6C8809(config-captive-portal-test)#
```

#### Related Commands

|           |                                                     |
|-----------|-----------------------------------------------------|
| <b>no</b> | Disables accounting records for this captive portal |
|-----------|-----------------------------------------------------|

#### bypass

Enables bypassing of captive portal detection requests from wireless clients

Certain devices, such as Apple iOS devices send CNA (Captive Network Assistant) requests to detect existence of captive portals. When enabled, the bypass option does not allow CNA requests to be redirected to the captive portal pages.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
bypass captive-portal-detection
```

#### Parameters

```
bypass captive-portal-detection
```

|                                 |                                            |
|---------------------------------|--------------------------------------------|
| bypass captive-portal-detection | Bypasses captive portal detection requests |
|---------------------------------|--------------------------------------------|

#### Examples

```
rfs4000-229D58(config-captive-portal-test)#bypass captive-portal-detection
rfs4000-229D58(config-captive-portal-test)#show context
aptive-portal test
bypass captive-portal-detection
rfs4000-229D58(config-captive-portal-test)#
```

#### Related Commands

|           |                                                         |
|-----------|---------------------------------------------------------|
| <b>no</b> | Disables bypassing of captive portal detection requests |
|-----------|---------------------------------------------------------|

#### connection-mode

Configures a captive portal's mode of connection to the Web server. HTTP uses plain unsecured connection for user requests. HTTPS uses an encrypted connection to support user requests.

Both HTTP and HTTPS use the same URI (Uniform Resource Identifier), so controller and client resources can be identified. However, the use of HTTPS is recommended, as it affords controller and client transmissions some measure of data protection HTTP cannot provide.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000

- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
connection-mode [http|https]
```

#### Parameters

```
connection-mode [http|https]
```

|                                                                                                                |                                                                        |
|----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| http                                                                                                           | Sets HTTP as the default connection mode. This is the default setting. |
| https                                                                                                          | Sets HTTPS as the default connection mode                              |
| <b>Note:</b> HTTPS is a more secure version of HTTP, and uses encryption while sending and receiving requests. |                                                                        |

#### Examples

```
nx9500-6C8809(config-captive-portal-test)#connection-mode https
nx9500-6C8809(config-captive-portal-test)#show context
captive-portal test
 access-type logging
 access-time 35
 connection-mode https
 accounting syslog host 172.16.10.13 port 1
nx9500-6C8809(config-captive-portal-test)#
```

#### Related Commands

|    |                                               |
|----|-----------------------------------------------|
| no | Removes this captive portal's connection mode |
|----|-----------------------------------------------|

### custom-auth

Configures custom user information

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
custom-auth info <LINE>
```

#### Parameters

```
custom-auth info <LINE>
```

|             |                                                                                                                                                                                                                                                                                                     |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| info <LINE> | Configures information used for RADIUS lookup when <i>custom-auth RADIUS</i> access type is configured <ul style="list-style-type: none"> <li>• &lt;LINE&gt; – Guest data needs to be provided. Specify the <i>name</i>, <i>e-mail address</i>, and <i>telephone number</i> of the user.</li> </ul> |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config-captive-portal-test)#custom-auth info bob bob@examplecompany.com
nx9500-6C8809(config-captive-portal-test)#show context
captive-portal test
 access-type logging
 access-time 35
 custom-auth info bob bob@examplecompany.com
 connection-mode https
```



```
accounting syslog host 172.16.10.13 port 1
nx9500-6C8809(config-captive-portal-test)#
```

#### Related Commands

|                                                                               |
|-------------------------------------------------------------------------------|
| <b>no</b> Removes custom user information configured with this captive portal |
|-------------------------------------------------------------------------------|

#### data-limit

Enforces data transfer limits on captive portal clients. This feature enables the tracking and logging of user usage. Users exceeding the allowed bandwidth are restricted from the captive portal.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
data-limit <1-102400> {action [log-and-disconnect|log-only]}
```

#### Parameters

```
data-limit <1-102400> {action [log-and-disconnect|log-only]}
```

|                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| data-limit<br><1-102400>             | Sets a captive portal client's data transfer limit in megabytes. This limit is applicable for both upstream and downstream data transfer. <ul style="list-style-type: none"><li>• &lt;1-102400&gt; – Specify a value from 1 - 102400 MB.</li></ul>                                                                                                                                                                                                                                                                                                |
| action [log-and-disconnect log-only] | Optional. Specifies the action taken when a client exceeds the configured data limit. The options are: <ul style="list-style-type: none"><li>• log-and-disconnect – When selected, an entry is added to the log file any time a captive portal client exceeds the data limit, and the client is disconnected.</li><li>• log-only – When selected, an entry is added to the log file any time a captive portal client exceeds the data limit. the client, however, remains connected to the captive portal. This is the default setting.</li></ul> |

#### Examples

```
rfs4000-229D58(config-captive-portal-test)#data-limit 200 action log-and-disconnect
rfs4000-229D58(config-captive-portal-test)#
rfs4000-229D58(config-captive-portal-test)#show context
captive-portal test
 data-limit 200 action log-and-disconnect
rfs4000-229D58(config-captive-portal-test)#
```

#### Related Commands

|                                                                     |
|---------------------------------------------------------------------|
| <b>no</b> Removes data limit enforcement for captive portal clients |
|---------------------------------------------------------------------|

#### frictionless-onboarding

Enables wireless clients, associated with guest WLANs, to self-register with the ExtremeGuest server. In other words, this feature enables frictionless on-boarding of guest users to the ExtremeGuest server.

It also provides an integration API, as a means of on-boarding guest users through a loyalty application.



#### Note

To enable this feature, in the Guest WLAN (using this captive-portal), enable MAC authentication and set the registration mode to 'device'. For information on enabling frictionless-onboarding, see [Examples](#) on page 302.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

`frictionless-onboarding`

#### Parameters

None

#### Examples

The following configurations are required to enable frictionless on-boarding of guest users to the ExtremeGuest server:

1 Create a captive-portal:

```
NX9500-EGuest(config)#captive-portal EGuest
NX9500-EGuest(config-captive-portal-EGuest)#
```

a Set the *access-type* as registration..

```
NX9500-WC-EGuest(config-captive-portal-EGuest)#access-type registration
```

This sets the guest user access and authentication mode to self-registration.

b Enable *frictionless-onboarding*.

```
NX9500-WC-EGuest(config-captive-portal-EGuest)#frictionless-onboarding
```

This enables auto-redirection of guest users to the ExtremeGuest server, where the user's MAC address is registered. Registered devices, on subsequent logins, are provided immediate access without interaction with Splash pages.

c Configure *Localization* URL..

```
NX9500-WC-EGuest(config-captive-portal-test)#localization fqdn local.guestaccess.com
```

When configured, the defined URL is triggered from a mobile application to derive location information from the wireless network so that an application can be localized to a particular store or region.

```
NX9500-WC-EGuest(config-captive-portal-Guest)#show context
captive-portal EGuest
 access-type registration
 webpage internal registration field city type text enable label "City" placeholder
 "Enter City"
 webpage internal registration field street type text enable label "Address"
 placeholder "123 Any Street"
 webpage internal registration field name type text enable label "Full Name"
 placeholder "Enter First Name, Last Name"
 webpage internal registration field zip type number enable label "Zip" placeholder
 "Zip"
 webpage internal registration field via-sms type checkbox enable title "SMS
 Preferred"
```

```

webpage internal registration field mobile type number enable label "Mobile"
placeholder "Mobile Number with Country code"
webpage internal registration field age-range type dropdown-menu enable label "Age
Range" title "Age Range"
webpage internal registration field email type e-address enable mandatory label
"Email" placeholder "you@domain.com"
webpage internal registration field via-email type checkbox enable title "Email
Preferred"
frictionless-onboarding
localization fqdn local.guestaccess.com
NX9500-WC-EGuest(config-captive-portal-Guest)#

```



**Note**

This is an example fqdn URI.

2 Create a WLAN with the following settings:

- a Set authentication-type as 'mac'.

```
NX9500-WC-EGuest(config-wlan-EGuest)#authentication-type mac
```

When configured, enables MAC authentication of guest users.

- b Enable device registration.

```
NX9500-WC-EGuest(config-wlan-EGuest)#registration device group-name test expiry-time
300
```

When enabled, guest users' device MAC addresses are registered in the database. Registered devices are provided immediate access on subsequent logins.

- c Set guest-registration as external.

```
NX9500-WC-EGuest(config-wlan-EGuest)#registration external follow-aaa
```

This enables forwarding of guest registration and authentication requests to an external authentication server resource, specified in an AAA policy.

Note, in this scenario, the external resource is the ExtremeGuest server.

Execute the command in the following step to specify the AAA Policy.

- d Apply an AAA Policy to the WLAN.

```
NX9500-WC-EGuest(config-wlan-EGuest)#use aaa-policy guest
```

When applied, registration and authentication requests are forwarded to the authentication server configured in the specified AAA Policy.



**Note**

In the AAA policy, ensure that the authentication server configuration points to the ExtremeGuest server.

- e Enable captive-portal enforcement.

```
NX9500-WC-EGuest(config-wlan-EGuest)#captive-portal-enforcement fall-back
```

When enabled, captive-portal validation is enforced on clients requesting access. Fall-back is an optional parameter that enforces captive-portal authentication only on failure of WLAN authentication.

- f Use the captive-portal configured in Step 1 in the WLAN..

```
NX9500-WC-EGuest(config-wlan-EGuest)#use captive-portal EGuest
```

```
NX9500-WC-EGuest(config-wlan-EGuest)#show context
```

```
wlan EGuest
```

```
ssid eguest
```

```

bridging-mode local
encryption-type none
authentication-type mac
use captive-portal EGuest
captive-portal-enforcement fall-back
registration device group-name test expiry-time 300
NX9500-WC-EGuest(config-wlan-EGuest)#

```

This is the captive-portal used with this WLAN for captive-portal validation of guest users.

#### Related Commands

|                                              |                                                                                        |
|----------------------------------------------|----------------------------------------------------------------------------------------|
| <code>no (captive-portal-config-mode)</code> | Disables frictionless-onboarding of guest users to the ExtremeGuest server on page 327 |
|----------------------------------------------|----------------------------------------------------------------------------------------|

#### inactivity-timeout

Defines an inactivity timeout in seconds. If a frame is not received from a client for the specified interval, the current session is terminated.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
inactivity-timeout <60-86400>
```

#### Parameters

```
inactivity-timeout <60-86400>
```

|                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>&lt;60-86400&gt; Defines the interval for which a captive portal session is kept alive without receiving a frame from the client. The session is automatically terminated once this interval is over.</p> <ul style="list-style-type: none"> <li>• &lt;60-86400&gt; – Specify a value from 60 - 86400 seconds. The default is 10 minutes or 600 seconds.</li> </ul> |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```

nx9500-6C8809(config-captive-portal-test)#inactivity-timeout 750
nx9500-6C8809(config-captive-portal-test)#show context
captive-portal test
 access-type logging
 access-time 35
 custom-auth info bob bob@examplecompany.com
 connection-mode https
 inactivity-timeout 750
 accounting syslog host 172.16.10.13 port 1
nx9500-6C8809(config-captive-portal-test)#

```

#### Related Commands

|                 |                                                                            |
|-----------------|----------------------------------------------------------------------------|
| <code>no</code> | Removes the client inactivity interval configured with this captive portal |
|-----------------|----------------------------------------------------------------------------|

#### ipv6

Configures the internal captive portal server's (running on the centralized mode) IPv6 address. If using centralized server mode, use this option to define the controller, service platform, or access point resource's (hosting the captive portal) IPv6 address. For information on configuring the server mode, see [server](#).

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
ipv6 server host <IPv6>
```

#### Parameters

```
ipv6 server host <IPv6>
```

|                         |                                                                                                                                                                                             |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ipv6 server host <IPv6> | Configures the IPv6 address of the internal captive portal server <ul style="list-style-type: none"><li>• &lt;IPv6&gt; - Specify the captive portal server's global IPv6 address.</li></ul> |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
rfs4000-229D58(config-captive-portal-test2)#ipv6 server host 2001:10:10:10:6d:33:fa:8b
rfs4000-229D58(config-captive-portal-test2)#show context
captive-portal test2
 access-type OAuth
 ipv6 server host 2001:10:10:10:6d:33:fa:8b
 OAuth client-id Google TechPubs.printer.google.com
rfs4000-229D58(config-captive-portal-test2)#
```

#### Related Commands

|           |                                                  |
|-----------|--------------------------------------------------|
| <b>no</b> | Removes the captive portal server's IPv6 address |
|-----------|--------------------------------------------------|

## localization

Configures an FQDN address string to get localization parameters for the client. Use this option to add a URL to trigger a one-time redirect on demand. The defined URL is triggered from a mobile application to derive location information from the wireless network so an application can be localized to a particular store or region.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
localization [fqdn <WORD>|response <WORD>]
```

#### Parameters

```
localization [fqdn <WORD>|response <WORD>]
```

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| localization    | Enables localization and configures the related parameters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| fqdn <WORD>     | Configures the FQDN address (for example, local.guestaccess.com) used to obtain localization parameters for a client. <ul style="list-style-type: none"> <li>&lt;WORD&gt; - Specify the FQDN address string. For example, local.guestaccess.com</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| response <WORD> | Configures the response message directed back to the client for localization HTTP requests. <ul style="list-style-type: none"> <li>&lt;WORD&gt; - Specify the response message (should not exceed 512 characters in length).</li> </ul> <p>The following built-in query tags can be included in the response message:</p> <p>'WING_TAG_CLIENT_IP' -Captive portal client IPv4 address</p> <p>'WING_TAG_CLIENT_MAC' - Captive portal client MAC address</p> <p>'WING_TAG_WLAN_SSID ' - Captive portal client WLAN ssid</p> <p>'WING_TAG_AP_MAC' - Captive portal client AP MAC address</p> <p>'WING_TAG_AP_NAME' - Captive portal client AP Name</p> <p>'WING_TAG_RF_DOMAIN' - Captive portal client RF Domain</p> <p>'WING_TAG_USERNAME' - Captive portal authentication username</p> <p>'WING_TAG_USERTYPE' - Captive portal usertype</p> <p>(new/return/refresh) Example:- &lt;local&gt;&lt;site&gt;WING_TAG_RF_DOMAIN&lt;/site&gt;&lt;ap&gt;WING_TAG_AP_NAME&lt;/ap&gt;&lt;/local&gt;</p> |

### Examples

```

nx9500-6C8809(config-captive-portal-test)#localization fqdn local.guestaccess.com
nx9500-6C8809(config-captive-portal-test)#localization response <local><site>SJExtreme</
site><ap>ap8163-74B45C</ap><user>Bob</user><local>
nx9500-6C8809(config-captive-portal-TechPubsNew)#show context
captive-portal TechPubsNew
 webpage internal registration field city type text enable label "City" placeholder "Enter
 City"
 webpage internal registration field street type text enable label "Address" placeholder
 "123 Any Street"
 webpage internal registration field name type text enable label "Full Name" placeholder
 "Enter First Name, Last Name"
 webpage internal registration field zip type number enable label "Zip" placeholder "Zip"
 webpage internal registration field via-sms type checkbox enable title "SMS Preferred"
 webpage internal registration field mobile type number enable label "Mobile" placeholder
 "Mobile Number with Country code"
 webpage internal registration field age-range type dropdown-menu enable label "Age Range"
 title "Age Range"
 webpage internal registration field email type e-address enable mandatory label "Email"
 placeholder "you@domain.com"
 webpage internal registration field via-email type checkbox enable title "Email Preferred"
 localization fqdn local.guestaccess.com
 localization response <local><site>SJExtreme</site><ap>ap8163-74B45C</ap><user>Bob</
 user><local>
nx9500-6C8809(config-captive-portal-TechPubsNew)#

```

### Related Commands

no

Removes the FQDN address string and response message configured on a captive portal for localization

## logout-fqdn

the Logout FQDN as the FQDN address to logout of the captive portal session from the client (for example, *logout.guest.com*).

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
logout-fqdn <WORD>
```

### Parameters

```
logout-fqdn <WORD>
```

logout-fqdn <WORD> Configures the FQDN address used to logout

- <WORD> – Provide the FQDN address (for example, *logout.guestaccess.com*).

### Examples

```
rfs4000-229D58(config-captive-portal-test)#logout-fqdn logout.testuser.com
rfs4000-229D58(config-captive-portal-test)#show context
captive-portal test
 logout-fqdn logout.testuser.com
rfs4000-229D58(config-captive-portal-test)#
```

### Related Commands

no

Clears the logout FQDN address

## oauth

Enables OAuth-driven Google and/or Facebook authentication on captive portals that use internal Web pages.

To enable Google and Facebook captive-portal authentication:

- Enforce captive-portal authentication on the WLAN to which wireless-clients associate. For information, see [captive-portal-enforcement](#).
- Set captive-portal Web page location to internal. For more information, see [webpage-location](#).
- Register your captive-portal individually on Google/FaceBook APIs and generate a client-id and client-secret. The client-ids retrieved during registration are the IDs for the WiNG application running on the access point/controller. The WiNG application uses these client-ids to access the Google and Facebook Auth APIs, and authenticate the guest client on behalf of the user.

If enabling OAuth-driven Google and/or Facebook authentication on the captive portal, use this command to configure the Google/Facebook client-ids. Once enabled, the captive portal landing page, displayed on the client's browser, provides the Facebook and Google login buttons.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
oauth
oauth client-id [facebook|google] <WORD>
```

## Parameters

```
oauth
```

|       |                                                                                                                                                                                                    |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| oauth | Execute this command without the associated keywords to enable OAuth on this captive-portal. If enabling OAuth, ensure the captive-portal Web page location is configured as advanced or external. |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
oauth client-id [facebook|google] <WORD>
```

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| oauth client-id [facebook google] <WORD> | <p>Configures the client-ids retrieved from the Google and Facebook API manager portals during registration</p> <ul style="list-style-type: none"> <li>• facebook - Configures the Facebook API client-id (is a 15 digit entity)</li> <li>• google - Configures the Google API client-id (is a 12 digit number) <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Provide the Facebook/Google client-id.</li> </ul> </li> </ul> <p>If the captive-portal Web page location is advanced or external, and you are enabling OAuth support, you need not configure the client-id. In such a scenario, the client-id is configured through the EGuest server UI and not the WiNG CLI.</p> |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Example (User Exec Mode)

```
nx7500-6DCD39(config-captive-portal-test2)#OAuth
nx7500-6DCD39(config-captive-portal-test2)#OAuth client-id Google
xxxxxxxxxxxxx.apps.googleusercontent.com Facebook yyyyyyyyyyyyyyyy
nx7500-6DCD39(config-captive-portal-test2)#show context
captive-portal test2
server host guest.social.com
oauth
oauth client-id Google xxxxxxxxxxxxxx.apps.googleusercontent.com Facebook yyyyyyyyyyyyyyyy

nx7500-6DCD39(config-captive-portal-test)#
```

In the above example,

- xxxxxxxxxxxxxx - Is the 12 digit numeric part of your Google client-id.
- yyyyyyyyyyyyyyyy - Is the 15 digit Facebook client-id

## Related Commands

|    |                                                                        |
|----|------------------------------------------------------------------------|
| no | Removes all OAuth client identities configured for this captive portal |
|----|------------------------------------------------------------------------|

## php-helper

Configures a PHP helper to serve the PHP splash pages to guest users logging in to the captive portal using social-media credentials. Configure a PHP helper only if the following criteria are fulfilled:

- OAuth-based authentication is enabled on the captive portal.
- The captive-portal server mode is "self".



- The access point, hosting the captive-portal server, has low memory space (for example, the AP 6522, and AP 7502 model access points).
- A hotspot server, hosting the captive-portal PHP splash pages, is up and running.

The WiNG software introduces HybridAuth support on captive portals. HybridAuth is an open-source, social-sign on PHP Library. In addition to Google and Facebook, it allows a variety of third-party social authentications, such as *LinkedIn*, *Twitter*, *Live*, *Yahoo*, *OpenID*, etc. However, HybridAuth uses space-consuming PHP splash pages that cannot be loaded on access points with low memory space. These access points can only serve the initial landing page, where guests clicking on a social login button are redirected by the php-helper to a PHP page hosted on the PHP-helper.

To create PHP splash pages, use the splash template configuration tool available on the EGuest (ExtremeGuest) dashboard. Upload the generated tar to both the hotspot server and the php helper. Note, the EGuest dashboard can be launched from the WiNG controller (NX 95XX/NX 96XX/VX 9000) enabled as the EGuest server.

For more information on enabling the EGuest server, see [eguest-server \(VX9000 only\)](#) on page 990.

For more information on configuring an EGuest captive portal, see [configuring ExtremeGuest captive portal](#) on page 332.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
php-helper [controller|domain-manager]
php-helper controller <IP/HOSTNAME> hosting-vlan-interface <0-4096>
php-helper domain-manager <IP/HOSTNAME>
```

#### Parameters

```
php-helper controller <IP/HOSTNAME> hosting-vlan-interface <0-4096>
```

|                                 |                                                                                                                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| php-helper                      | Configures the php-helper parameters                                                                                                                                                                                      |
| controller <IP/HOSTNAME>        | Configures the controller adopting the captive-portal access point as the php-helper <ul style="list-style-type: none"> <li>• &lt;IP/HOSTNAME&gt; - Specify the adopting controller's IP address or host name.</li> </ul> |
| hosting-vlan-interface <0-4096> | Optional. Configures the VLAN on which the php-helper is reachable <ul style="list-style-type: none"> <li>• &lt;0-4096&gt; - Specify the VLAN hosting the php-helper from 0 - 4096.</li> </ul>                            |

```
php-helper domain-manager <IP/HOSTNAME>
```

|                              |                                                                                                                                                                                                                     |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| php-helper                   | Configures the php-helper parameters                                                                                                                                                                                |
| domain-manager <IP/HOSTNAME> | Configures the captive-portal access point's RF Domain manager as the php-helper <ul style="list-style-type: none"> <li>• &lt;IP/HOSTNAME&gt; - Specify the RF Domain manager's IP address or host name.</li> </ul> |

#### Examples

To enable php-helper configure the following parameters in the captive-portal context:

```
ap6532-3163A4(config-captive-portal-php-helper)#oauth
ap6532-3163A4(config-captive-portal-php-helper)#php-helper controller nx9500-6C8809
ap6532-3163A4(config-captive-portal-php-helper)#server mode self
ap6532-3163A4(config-captive-portal-php-helper)#server host cpsocial.extreme.com
```

Note, when configuring the server, specify the server's hostname and not the IP address, because some social media do not allow IP address as a redirect URI.

```
ap6532-3163A4(config-captive-portal-php-helper)#show running-config captive-portal php-
helper
captive-portal php-helper
 server host cpsocial.extreme.com
 php-helper controller nx9500-6C8809
 oauth
 webpage internal registration field city type text enable label "City" placeholder "Enter
 City"
 webpage internal registration field street type text enable label "Address" placeholder
 "123 Any Street"
 webpage internal registration field name type text enable label "Full Name" placeholder
 --More--
ap6532-3163A4(config-captive-portal-php-helper)#
```

#### Related Commands

|                 |                                      |
|-----------------|--------------------------------------|
| <code>no</code> | Removes the PHP helper configuration |
|-----------------|--------------------------------------|

#### post-authentication-vlan

Configures the VLAN that is assigned to this captive portal's users upon successful authentication

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
post-authentication-vlan [<1-4096> | <VLAN-ALIAS>]
```

#### Parameters

```
post-authentication-vlan [<1-4096> | <VLAN-ALIAS>]
```

|                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>post-authentication-vlan [<b>&lt;1-4096&gt;</b>   <b>&lt;VLAN-ALIAS&gt;</b>]</code> | Configures the post authentication VLAN. The VLAN specified here is assigned to this captive portal's users after they have authenticated and logged on to the network. Provide the VLAN ID, or use an existing VLAN alias to identify the post authentication VLAN. <ul style="list-style-type: none"><li>• <b>&lt;1-4096&gt;</b> – Specify the VLAN's number from 1 - 4096.</li><li>• <b>&lt;VLAN-ALIAS&gt;</b> – Specify the VLAN alias (should be existing and configured). VLAN alias names begin with a '\$'.</li></ul> |
|-------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Example

```
rfs4000-229D58(config-captive-portal-test)#post-authentication-vlan 1
rfs4000-229D58(config-captive-portal-test)#show context
captive-portal test
 post-authentication-vlan 1
rfs4000-229D58(config-captive-portal-test)#
```

#### Related Commands

**no** Removes the post authentication RADIUS VLAN assigned to this captive portal's users

•

## radius-vlan-assignment

Enables assignment of a RADIUS VLAN for this captive portal

When enabled, if the RADIUS server as part of the authentication process returns a client's VLAN-ID in a RADIUS access-accept packet, then all client traffic is forwarded on the post authentication VLAN. If disabled, the RADIUS server's VLAN assignment is ignored and the VLAN configuration defined within the WLAN configuration is used instead. This feature is disabled by default.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
radius-vlan-assignment
```

### Parameters

None

### Example

```
rfs4000-229D58(config-captive-portal-test)#radius-vlan-assignment
rfs4000-229D58(config-captive-portal-test)#show context
captive-portal test
 post-authentication-vlan 1
 radius-vlan-assignment
rfs4000-229D58(config-captive-portal-test)#
```

### Related Commands

**no** Disables assignment of a RADIUS VLAN for this captive portal

## redirection

Configures a list of destination ports (separated by commas, or using a dash for a range) that are taken into consideration when redirecting client connections

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
redirection ports <LIST-OF-PORTS>
```

### Parameters

```
redirection ports <LIST-OF-PORTS>
```

|                       |                                                                                                                                                                                                                                                                          |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ports <LIST-OF-PORTS> | Configures destination ports considered for redirecting client connection<br>A maximum of 16 ports can be specified in a comma-separated list. Standard ports 80 and 443 are always considered for client connections regardless of what's entered by the administrator. |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Example

```
rfs4000-229D58(config-captive-portal-test)#redirection ports 1,2,3
rfs4000-229D58(config-captive-portal-test)#show context
captive-portal test
 redirection ports 1-3
rfs4000-229D58(config-captive-portal-test)#
```

#### Related Commands

|    |                                           |
|----|-------------------------------------------|
| no | Disables redirection of client connection |
|----|-------------------------------------------|

### report-royalty-application

Enables detection of captive portal client's usage of a selected (preferred) loyalty application

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
report-loyalty-application {custom-app <APPLICATION-NAME>}
```

#### Parameters

```
report-loyalty-application {custom-app <APPLICATION-NAME>}
```

|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| report-loyalty-application {custom-app <APPLICATION-NAME>} | <p>Reports a captive portal client's loyalty application presence and stores this information in the captive portal's user database. The client's loyalty application detection occurs on the access point to which the client is associated. Retail administrators can use this information to assess whether patrons' loyalty application usage is as per expectation within specific retail environments. This option is disabled by default.</p> <ul style="list-style-type: none"><li>• custom-app &lt;APPLICATION-NAME&gt; - Optional. Uses a custom application definition as match criteria.</li><li>• &lt;APPLICATION-NAME&gt; - Specify the custom application name (should be existing and configured). Ensure that the application specified is available and configured. If not, create an application definition. For more information, see <a href="#">application</a>.</li></ul> <p>If no custom application definition is specified, the system uses localization to detect application presence.</p> |
|------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config-captive-portal-test)#report-loyalty-application custom-app
AntiVirus
nx9500-6C8809(config-captive-portal-test)#show context include-factory | include
report-loyalty-application
 report-loyalty-application custom-app AntiVirus
nx9500-6C8809(config-captive-portal-test)#
```

#### Related Commands

|    |                                                             |
|----|-------------------------------------------------------------|
| no | Disables detection of customer-loyalty application presence |
|----|-------------------------------------------------------------|

## server

Configures captive portal server parameters, such as the hostname, IP address, and mode of operation. This is the captive-portal server hosting the captive portal Web pages.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
server [host | mode]
server host <IP/HOSTNAME>
server mode [centralized|centralized-controller {hosting-vlan-interface <0-4096>}|self]
```

### Parameters

```
server host <IP/HOSTNAME>
```

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| host <IP/<br>HOSTNAME> | <p>Configures the internal captive portal server (wireless controller, access point, service platform)</p> <ul style="list-style-type: none"> <li>• &lt;IP/HOSTNAME&gt; – Specify the IPv4/IPv6 address or hostname of the captive portal server.</li> </ul> <p>For centralized-controller mode, the server host should be a virtual hostname and not an IP address.</p> <p>If enabling OAuth (social-media login) on the captive portal, configure the server's hostname and not the IP address. This is because some social media do not allow IP address as redirect-uri. For more information, see <a href="#">oauth</a> and <a href="#">php-helper</a>.</p> |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
server mode [centralized|centralized-controller {hosting-vlan-interface <0-4096>}|self]
```

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mode        | <p>Configures the captive portal server mode. This parameter identifies the device that will capture and redirect a wireless user's Web browser session to a landing page where the user has to provide login credentials in order to access the managed network. The WiNG captive portal implementation is very flexible and allows captive portal services to reside anywhere within the WiNG managed network. For example, the capture and redirection can be performed directly by the access points at the edge of the network, centrally on the controllers or service platforms managing the access points, or on dedicated wireless controller deployed within an isolated network.</p> |
| centralized | <p>Select this option if capture and redirection is provided by a designated wireless controller/service platform on the network defined using an IPv4/IPv6 address or hostname. This dedicated device can either be managing the dependent/independent access points or be a dedicated device deployed over the intermediate network.</p> <p>Ensure the IPv4 address or hostname of the WiNG wireless controller performing the capture and redirection is defined in the captive portal policy. And also, that the wireless controller is reachable via MINT.</p>                                                                                                                             |

|                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| centralized-controller {hosting-vlan-interface <0-4096>} | <p>Select this option if capture and redirection is on a cluster of wireless controller/service platforms managing dependent/independent access points when redundancy is required. The capture and redirection is provided by one of the controllers in the cluster that is operating as the designated forwarder for the tunneled VLAN. The cluster can be configured as active/active or active/standby as required.</p> <p>If using this option, ensure a non-resolvable virtual hostname is defined in the captive portal policy which is shared between the controllers in the cluster.</p> <ul style="list-style-type: none"> <li>hosting-vlan-interface – Optional. Configures the VLAN where the client can reach the captive-portal server. This option is available only for the centralized-controller mode. <ul style="list-style-type: none"> <li>&lt;0-4096&gt; – Specify the VLAN number (0 implies the controller is available on the client's VLAN).</li> </ul> </li> </ul> |
| self                                                     | <p>Select this option if capture and redirection is provided by the access point that is servicing the captive portal enabled Wireless LAN. This is the default setting.</p> <p>When enabled each remote access point servicing the captive portal enabled WLAN performs the captive portal capture and redirection internally. The WLAN users are mapped to a locally bridged VLAN for which each access point has a SVI defined. The SVI can either have a static or dynamic (DHCP) IPv4 address assigned. The capture, redirection, and presentation of the captive portal pages are performed using the SVI on each access point the wireless device is associated to.</p>                                                                                                                                                                                                                                                                                                                |

### Examples

```

nx9500-6C8809(config-captive-portal-test)#server host 172.16.10.9
nx9500-6C8809(config-captive-portal-test)#show context
captive-portal test
 access-time 35
 custom-auth info bob bob@examplecompany.com
 connection-mode https
 inactivity-timeout 750
 server host 172.16.10.9
nx9500-6C8809(config-captive-portal-test)#

```

### Related Commands

|           |                                                          |
|-----------|----------------------------------------------------------|
| <b>no</b> | Resets or disables captive portal host and mode settings |
|-----------|----------------------------------------------------------|

### simultaneous-users

Specifies the number of users (client MAC addresses) that can simultaneously log on to the captive portal. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
simultaneous-users <1-8192>
```

### Parameters

```
simultaneous-users <1-8192>
```

|                             |                                                                                                                                                                                                  |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| simultaneous-users <1-8192> | <p>Specifies the number of MAC addresses that can simultaneously access the captive portal</p> <ul style="list-style-type: none"> <li>&lt;1-8192&gt; – Select a number from 1 - 8192.</li> </ul> |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-captive-portal-test)#simultaneous-users 5
nx9500-6C8809(config-captive-portal-test)#show context
captive-portal test
 access-time 35
 custom-auth info bob bob@examplecompany.com
 connection-mode https
 inactivity-timeout 750
 server host 172.16.10.9
 simultaneous-users 5
nx9500-6C8809(config-captive-portal-test)#
```

## Related Commands

|           |                                            |
|-----------|--------------------------------------------|
| <b>no</b> | Resets or disables captive portal commands |
|-----------|--------------------------------------------|

## terms-agreement

Enforces the user to agree to terms and conditions (included in the login page) for captive portal access. This feature is disabled by default.

When enabled, the system enforces a previously registered user to re-confirm the terms of agreement, on successive log ins, only if the interval between the last log out and the current log in exceeds the agreement-refresh timeout configured in the WLAN context. For more information on configuring the agreement-refresh timeout value, see [registration](#).

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
terms-agreement
```

## Parameters

None

## Examples

```
nx9500-6C8809(config-captive-portal-test)#terms-agreement
nx9500-6C8809(config-captive-portal-test)#show context
captive-portal test
 access-time 35
 custom-auth info bob bob@examplecompany.com
 connection-mode https
 inactivity-timeout 750
 server host 172.16.10.9
 simultaneous-users 5
 terms-agreement
nx9500-6C8809(config-captive-portal-test)#
```

## Related Commands

|           |                                            |
|-----------|--------------------------------------------|
| <b>no</b> | Resets or disables captive portal commands |
|-----------|--------------------------------------------|

use (captive-portal-config-mode)

Configures a AAA policy and DNS whitelist with this captive portal policy. AAA policies are used to configure authentication and accounting servers for this captive portal. DNS whitelists restrict users to a set of configurable domains on the Internet.

For more information on AAA policies, see [aaa-policy](#).

For more information on DNS whitelists, see [dns-whitelist](#).

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
use [aaa-policy <AAA-POLICY-NAME>|dns-whitelist <DNS-WHITELIST-NAME>]
```

#### Parameters

```
use [aaa-policy <AAA-POLICY-NAME>|dns-whitelist <DNS-WHITELIST-NAME>]
```

|                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| aaa-policy <AAA-POLICY-NAME>       | Associates a AAA policy with this captive portal. AAA policies validate user credentials and provide captive portal access to the network. <ul style="list-style-type: none"><li>• &lt;AAA-POLICY-NAME&gt; - Specify the AAA policy name.</li></ul>                                                                                                                                                                                                           |
| dns-whitelist <DNS-WHITELIST-NAME> | Associates a DNS whitelist to use with this captive portal. A DNS whitelist defines a set of allowed destination IP addresses. DNS whitelists restrict captive portal access. <ul style="list-style-type: none"><li>• &lt;DNS-WHITELIST-NAME&gt; - Specify the DNS whitelist name.</li></ul> <p>To effectively host captive portal pages on an external Web server, the IP address of the destination Web server(s) should be added to the DNS whitelist.</p> |

#### Examples

```
nx9500-6C8809(config-captive-portal-test)#use aaa-policy test
nx9500-6C8809(config-captive-portal-test)#use dns-whitelist test
nx9500-6C8809(config-captive-portal-test)#show context
captive-portal test
 access-time 35
 custom-auth info bob bob@examplecompany.com
 connection-mode https
 inactivity-timeout 750
 server host 172.16.10.9
 simultaneous-users 5
 terms-agreement
 use aaa-policy test
 use dns-whitelist test
nx9500-6C8809(config-captive-portal-test)#
```

#### Related Commands

|           |                                                                 |
|-----------|-----------------------------------------------------------------|
| <b>no</b> | Removes a DNS Whitelist or a AAA policy from the captive portal |
|-----------|-----------------------------------------------------------------|

- 

#### webpage

Use this command to define the appearance and flow of Web pages requesting clients encounter when accessing a controller, service platform, or access point managed captive portal. Define whether the



Web pages are maintained locally or externally to the managing device as well as messages displayed requesting clients.

Configures Web pages displayed when interacting with a captive portal. There are six (6) different pages.

- acknowledgment – This page displays details for the user to acknowledge.
- agreement – This page displays “Terms and Conditions” that a user accepts before allowed access to the captive portal.
- fail – This page is displayed when the user is not authenticated.
- login – This page is displayed when the user connects to the captive portal. It fetches login credentials from the user.
- no-service – This page is displayed when a captive portal user is unable to access the captive portal due unavailability of critical services.
- registration – This page is displayed when users are redirected to a Web page where they have to register in the captive portal’s database.
- welcome – This page is displayed to welcome an authenticated user to the captive portal.

These Web pages, which interact with captive portal users, can be located either on the controller or an external location.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
webpage [external|internal]
webpage external [acknowledgment|agreement|fail|login {post}|no-service|
registration|welcome] <URL>
webpage internal [acknowledgment|agreement|fail|login|no-service|org-name|org-signature|
registration|welcome]
webpage internal [acknowledgment|agreement|fail|login|no-service|registration|welcome]
[description|footer|header|title] <CONTENT>
webpage internal [acknowledgment|agreement|fail|login|no-service|registration|welcome]
[body-background-color|body-font-color|org-background-color|org-font-color] <WORD>
webpage internal [acknowledgment|agreement|fail|login|no-service|registration|welcome]
[main-logo use-as-banner|small-logo] <URL>
webpage internal registration field [age-range|city|country|custom|disclaimer|dob|
email|gender|member|mobile|name|optout|street|via-email|via-sms|zip] type [checkbox|
date|
dropdown-menu|e-address|number|radio-button|text] enable
{label <LINE>/mandatory/title <LINE>/placeholder <LINE>}
webpage internal welcome use-external-success-url
webpage internal [org-name|org-signature] <LINE>
```

### Parameters

```
webpage external [acknowledgment|agreement|fail|login {post}|no-service|
registration|welcome] <URL>
```

|                |                                                                                                                                            |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| external       | Indicates Web pages being served are hosted on an external (to the captive portal) server resource                                         |
| acknowledgment | Indicates the page is displayed for user acknowledgment of details. Users are redirected to this page to acknowledge information provided. |

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| agreement    | <p>Indicates the page is displayed for “Terms &amp; Conditions”</p> <p>The agreement page provides conditions that must be agreed to before captive portal access is permitted.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| fail         | <p>Indicates the page is displayed for login failure</p> <p>The fail page asserts authentication attempt has failed, the user is not allowed to access the Internet (using this captive portal) and must provide the correct login information again to access the Internet.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| login {post} | <p>Indicates the page is displayed for getting user credentials. This page is displayed by default.</p> <ul style="list-style-type: none"> <li>• post – Optional. Redirects users to post externally when they during authentication</li> </ul> <p>The login page prompts the user for a username and password to access the captive portal and proceed to either the agreement page (if used) or the welcome page.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| no-service   | <p>Indicates the page is displayed when certain critical services are unavailable and the user fails to access the captive portal. The no-service page asserts the captive portal service is temporarily unavailable due to technical reasons. Once the services become available, the captive portal user is automatically connected back to the services available through the captive portal. The possible scenarios are:</p> <ul style="list-style-type: none"> <li>• The RADIUS server (on-board or external) is not reachable and the user cannot be authenticated</li> <li>• The external captive portal server is not reachable</li> <li>• The connectivity between the adopted AP and controller is lost</li> <li>• The external DHCP server is not reachable</li> </ul> <p>To provide this service, enable the following:</p> <ul style="list-style-type: none"> <li>• External captive portal server monitoring.</li> <li>• AAA server monitoring. This enables detection of RADIUS server failure.</li> <li>• External DHCP server monitoring.</li> <li>• AP to controller connectivity monitoring.</li> </ul> <p>For more information on enabling these critical resource monitoring, see <a href="#">service</a>.</p> |
| registration | <p>Indicates the page is displayed when users are redirected to a Web page where they have to register in the captive portal’s database.</p> <p>Guest users are redirected to an internally (or) externally hosted registration page (registration.html) upon association to a captive portal SSID, where previously, not-registered guest users can register.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| welcome | Indicates the page is displayed after a user has been successfully authenticated<br>The welcome page asserts a user has logged in successfully and can access the captive portal.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <URL>   | Indicates the URL to the Web page displayed. Query String: URL can include query tags.<br>Supported Query Tags are:<br>'WING_TAG_CLIENT_IP' - Captive portal client IPv4 address<br>'WING_TAG_CLIENT_MAC' - Captive portal client MAC address<br>'WING_TAG_WLAN_SSID' - Captive portal client WLAN ssid<br>'WING_TAG_AP_MAC' - Captive portal client AP MAC address<br>'WING_TAG_AP_NAME' - Captive portal client AP Name<br>'WING_TAG_RF_DOMAIN' - Captive portal client RF Domain<br>'WING_TAG_CP_SERVER' - Captive portal server address<br>'WING_TAG_USERNAME' - Captive portal authentication username<br>Example:<br>http://cportal.com/policy/login.html?client_ip=WING_TAG_CLIENT_IP&ap_mac=WING_TAG_AP_MAC.<br>Use '&' or '?' character to separate field-value pair.<br>Enter 'ctrl-v' followed by '?' to configure query string |

`webpage internal [acknowledgment|agreement|fail|login|no-service|registration|welcome] [description|footer|header|title] <CONTENT>`

|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| internal       | Indicates the Web pages are hosted on an internal server resource. This is the default setting.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| acknowledgment | Indicates the Web page is displayed for users to acknowledge the information provided                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| agreement      | Indicates the page is displayed for “Terms & Conditions”                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| fail           | Indicates the page is displayed for login failure                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| login          | Indicates the page is displayed for entering user credentials                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| no-service     | Indicates the page is displayed when certain critical services are unavailable and the user fails to access the captive portal. The possible scenarios are: <ul style="list-style-type: none"> <li>• The RADIUS server (on-board or external) is not reachable and the user cannot be authenticated</li> <li>• The external captive portal server is not reachable</li> <li>• The connectivity between the adopted AP and controller is lost</li> <li>• The external DHCP server is not reachable</li> </ul> To provide this service, enable the following: <ul style="list-style-type: none"> <li>• External captive portal server monitoring.</li> <li>• AAA server monitoring. This enables detection of RADIUS server failure.</li> <li>• External DHCP server monitoring.</li> <li>• AP to controller connectivity monitoring.</li> </ul> For more information on enabling these critical resource monitoring, see <a href="#">service</a> . |
| registration   | Indicates the page is displayed when users are redirected to a Web page where they have to register in the captive portal’s database<br>Guest users are redirected to an internally (or) externally hosted registration page (registration.html) upon association to a captive portal SSID, where previously, not-registered guest users can register.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| welcome        | Indicates the page is displayed after a user has been successfully authenticated                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| description    | Indicates the content is the description portion of each of the following internal Web pages: acknowledgment, agreement, fail, login, no-service, and welcome                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

|           |                                                                                                                                                                                                                                                                                                                                                         |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| footer    | Indicates the content is the footer portion of each of the following internal Web pages: acknowledgment, agreement, fail, no-service, registration, and welcome page. The footer portion contains the signature of the organization that hosts the captive portal.                                                                                      |
| header    | Indicates the content is the header portion of each of the following internal Web pages: acknowledgment, agreement, fail, no-service, and welcome page. The header portion contains the heading information for each of these pages.                                                                                                                    |
| title     | Indicates the content is the title of each of the following internal Web pages: acknowledgment, agreement, fail, no-service, and welcome page. The title for each of these pages is configured here.                                                                                                                                                    |
| <CONTENT> | The following keyword is common to all of the above internal Web page options: <ul style="list-style-type: none"> <li>• &lt;CONTENT&gt; – Specify the content displayed for each of the different components of the internal Web page. Enter up to 900 characters for the description and 256 characters each for header, footer, and title.</li> </ul> |

```
webpage internal [acknowledgment|agreement|fail|login|no-service|registration|welcome]
[main-logo use-as-banner|small-logo] <URL>
```

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| internal                | Indicates the Web pages are hosted on an internal server resource                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| acknowledgment          | Indicates the Web page is displayed for users to acknowledge the information provided                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| agreement               | Indicates the page is displayed for “Terms & Conditions”                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| fail                    | Indicates the page is displayed for login failure                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| login                   | Indicates the page is displayed for user credentials                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| no-service              | Indicates the page is displayed when certain critical services are unavailable and the user fails to access the captive portal. The possible scenarios are: <ul style="list-style-type: none"> <li>• The RADIUS server (on-board or external) is not reachable and the user cannot be authenticated</li> <li>• The external captive portal server is not reachable</li> <li>• The connectivity between the adopted AP and controller is lost</li> <li>• The external DHCP server is not reachable</li> </ul> <p>To provide this service, enable the following:</p> <ul style="list-style-type: none"> <li>• External captive portal server monitoring.</li> <li>• AAA server monitoring. This enables detection of RADIUS server failure.</li> <li>• External DHCP server monitoring.</li> <li>• AP to controller connectivity monitoring.</li> </ul> <p>For more information on enabling these critical resource monitoring, see <a href="#">service</a>.</p> |
| registration            | Indicates the page displayed is the registration page to which users are redirected in order to register in the captive portal's database<br>Guest users are redirected to an internally (or) externally hosted registration page (registration.html) upon association to a captive portal SSID, where previously, not-registered guest users can register.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| welcome                 | Indicates the page is displayed after a user has been successfully authenticated                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| main-logo use-as-banner | The following keyword is common to all of the above internal Web page options: <ul style="list-style-type: none"> <li>• main-logo – Indicates the main logo displayed in the header of each Web page</li> <li>• use-as-banner – Uses the image, specified here, as the Web page banner, in place of the logo and organization name</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

|            |                                                                                                                                                                                                                                                                                                                                                             |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| small-logo | <p>The following keyword is common to all of the above internal Web page options:</p> <ul style="list-style-type: none"> <li>• small-logo - Indicates the logo image displayed in the footer portion of each Web page, and constitutes the organization's signature</li> </ul>                                                                              |
| <URL>      | <p>This parameter is common to the 'main-logo' and 'small-logo' keywords and provides the complete URL from where the main-logo and small-logo files are loaded and subsequently cached on the system.</p> <ul style="list-style-type: none"> <li>• &lt;URL&gt; - Specify the location and name of the main-logo and the small-logo image files.</li> </ul> |

```
webpage internal registration field [age-range|city|country|custom|disclaimer|
dob|email|gender|member|mobile|name|optout|street|via-email|via-sms|zip]
type [checkbox|date|dropdown-menu|e-address|number|radio-button|text] enable
{label <LINE>/mandatory|title <LINE>/placeholder <LINE>}
```

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| internal     | Indicates the Web pages are hosted on an internal server resource                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| registration | <p>Allows you to customize the user registration page. Select this option if the captive-portal's access-type is set to registration. Use the field and type options to define the input fields (for example, age-range, city, email, etc.) and the field type (for example, text, checkbox, dropdown-menu, radio-button, etc.)</p> <p>Guest users are redirected to an internally (or) externally hosted registration page (registration.html) upon association to a captive portal SSID, where previously, not-registered guest users can register.</p> <p>If the registration Web page is not customized, the built-in, default registration page is displayed to the client.</p> |

field [age-range| city|country|  
custom| disclaimer| dob|email|  
gender|member| mobile|name|  
optout| street|via-email|via-sms|  
zip]

Configures the captive portal's registration page fields  
Following are the available fields and the field type for each:

- age-range – Creates the age-range input field (enabled by default and included in the built-in registration page)
  - dropdown-menu – Configures the age-range field as a drop-down menu
  - radio-button – Configures the age-range field as a radio button menu
- city – Creates the postal address: city name input field (enabled by default and included in the built-in registration page)
  - text – Configures the city field as only alpha-numeric and special characters input field
- country – Creates the postal address: country name input field (disabled by default)
  - text – Configures the country field as only alpha-numeric and special characters input field
- custom <WORD> – Creates a customized field (as per your requirement). Use the 'custom' option to create a field not included in the built-in list.
  - <WORD> – Provide a name for the field. On the registration page, the field is displayed under the name specified here.
- disclaimer – Creates client's disclaimer-confirmation input field (disabled by default)
- checkbox – Configures the disclaimer field as a check box
- dob – Creates the client's date of birth (DoB) input field (disabled by default)
  - date – Configures the DoB field as only date-format input field
  - dropdown-menu – Configures the DoB field as a drop-down menu
  - text – Configures the DoB field as only alpha-numeric and special characters input field
- email – Creates the e-mail address input field (enabled by default and included in the built-in registration page)
  - e-address – Configures the e-mail field as only e-mail address format input field
- gender – Creates client's gender input field (disabled by default)
  - dropdown-menu – Configures the gender field as a drop-down menu
  - radio-button – Configures the gender field as a radio button menu
- member – Creates client's loyalty or captive-portal membership card number input field (disabled by default)
  - number – Configures the member field as only-numeric characters input field
  - text – Configures the member field as only alpha-numeric and special characters input field
- mobile – Creates the mobile number input field (enabled by default and included in the built-in registration page)
  - number – Configures the mobile field as only-numeric characters input field
  - text – Configures the mobile field as only alpha-numeric and special characters input field
- name – Creates the client name input field (enabled by default and included in the built-in registration page)
  - text – Configures the name field as only alpha-numeric and special characters input field

|                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                             | <ul style="list-style-type: none"> <li>• optout – Creates an input field that enables clients to opt out from registering <ul style="list-style-type: none"> <li>• checkbox – Configures the optout field as a check box</li> </ul> </li> <li>• street – Creates the postal address: street name/number input field (enabled by default and included in the built-in registration page) <ul style="list-style-type: none"> <li>• text – Configures the street field as only alpha-numeric and special characters input field</li> </ul> </li> <li>• via-email – Creates the client’s preferred mode of communication as e-mail input field (enabled by default and included in the built-in registration page) <ul style="list-style-type: none"> <li>• checkbox – Configures the via-email field as a check box</li> </ul> </li> <li>• via-sms – Creates the client’s preferred mode of communication as SMS input field (enabled by default and included in the built-in registration page) <ul style="list-style-type: none"> <li>• checkbox – Configures the via-sms field as a check box</li> </ul> </li> <li>• zip – Creates the postal address: zip input field (enabled by default and included in the built-in registration page) <ul style="list-style-type: none"> <li>• number – Configures the zip field as only-numeric characters input field</li> <li>• text – Configures the zip field as only alpha-numeric and special characters input field</li> </ul> </li> </ul> |
| <p>type [checkbox date dropdown-menu e-address number radio-button text]</p>                | <p>After specifying the field, configure the field type. The options displayed depend on the field selected in the previous step. These options are: checkbox, date, dropdown-menu, e-address, number, radio-button, and text.</p> <ul style="list-style-type: none"> <li>• checkbox – Configures the field as a check box</li> <li>• date – Configures the field as only date-format input field</li> <li>• dropdown-menu – Configures the field as a drop-down menu</li> <li>• e-address – Configures the field as an e-mail address input field</li> <li>• number – Configures the field as only-numeric characters input field</li> <li>• radio-button – Configures the field as a radio button</li> <li>• text – Configures the field as only alpha-numeric and special characters input field</li> </ul> <p>Some of the fields can have more than one field type options. For example, the field 'zip' can either be a numerical field or a text. Select the one best suited for your captive-portal.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <p>enable {label &lt;LINE&gt;  mandatory  title &lt;LINE&gt;  placeholder &lt;LINE&gt;}</p> | <p>Enables the field. When enabled, the field is displayed on the registration page. After enabling the field, optionally configure the following parameters:</p> <ul style="list-style-type: none"> <li>• label &lt;LINE&gt; – Optional. Configures the field’s label</li> <li>• mandatory – Optional. Makes the field mandatory</li> <li>• title – Optional. Configures the comma-separated list of items to include in the drop-down menu.</li> <li>• placeholder &lt;LINE&gt; – Optional. Configures a string, not exceeding 300 characters, that is displayed within the field. If not configured, the field remains blank.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

webpage internal welcome use-external-success-url



|                          |                                                                                                                                                                                                                                                                         |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| internal                 | Indicates the Web pages are hosted on an internal server resource                                                                                                                                                                                                       |
| welcome                  | Indicates the page is displayed after a user has been successfully authenticated                                                                                                                                                                                        |
| use-external-success-url | When configured, redirects the user, on successful authentication, to an externally hosted success URL from the locally-hosted landing page.<br>Use the <b>webpage &gt; external &gt; welcome &gt; &lt;URL&gt;</b> command to specify the location of the Welcome page. |

```
webpage internal [org-name|org-signature] <LINE>
```

|               |                                                                                                             |
|---------------|-------------------------------------------------------------------------------------------------------------|
| internal      | Indicates the Web pages are hosted on an internal server resource                                           |
| org-name      | Specifies the company's name, included on Web pages along with the main image                               |
| org-signature | Specifies the company's signature information, included in the bottom of Web pages along with a small image |
| <LINE>        | Specify the company's name or signature depending on the option selected.                                   |

### Examples

```
nx9500-6C8809(config-captive-portal-guest)#webpage external welcome http://192.168.9.46/welcome.html
nx9500-6C8809(config-captive-portal-guest)#show context
captive-portal guest
webpage external welcome http://192.168.9.46/welcome.html
nx9500-6C8809(config-captive-portal-guest)#
nx9500-6C8809(config-captive-portal-register)#webpage internal registration field age-range type dropdown-menu enable mandatory title 10-20,20-30,30-40,50-60,60-70
nx9500-6C8809(config-captive-portal-register)#show context include-factory | include age-range
 webpage internal registration field age-range type dropdown-menu enable mandatory label "Age Range" title "10-20,20-30,30-40,50-60,60-70"
nx9500-6C8809(config-captive-portal-register)#
```

In the following examples, the background and font colors have been customized for the captive portal's login page. Similar customizations can be applied to the acknowledgement, agreement, fail, welcome, no-service, and registration captive portal pages.

```
nx9500-6C88099(config-captive-portal-cap-enhanced-policy)#webpage internal login
body-background-color #E7F0EB
nx9500-6C8809(config-captive-portal-cap-enhanced-policy)#webpage internal login
body-font-color #EF68A7
nx9500-6C8809(config-captive-portal-cap-enhanced-policy)#webpage internal login
org-background-color #EFE4E9
nx9500-6C8809(config-captive-portal-cap-enhanced-policy)#webpage internal login
org-font-color #BA4A21
nx9500-6C8809(config-captive-portal-cap-enhanced-policy)#show context
captive-portal cap-enhanced-policy
 webpage internal login org-background-color #EFE4E9
 webpage internal login org-font-color #BA4A21
 webpage internal login body-background-color #E7F0EB
 webpage internal login body-font-color #EF68A7
nx9500-6C8809(config-captive-portal-cap-enhanced-policy)#
```



The following examples configure a scenario where a successfully authenticated user is redirected to an externally hosted Welcome page from the internal landing page.

```
nx9500-6C8809(config-captive-portal-cap-enhanced-policy)#webpage external welcome http://192.168.13.10/WelcomePage.html
nx9500-6C8809(config-captive-portal-cap-enhanced-policy)#webpage internal welcome use-external-success-url
nx9500-6C8809(config-captive-portal-cap-enhanced-policy)#show context
captive-portal cap-enhanced-policy
 webpage external welcome http://192.168.13.10/WelcomePage.html
 webpage internal acknowledgement org-background-color #33ff88
 webpage internal acknowledgement org-font-color #bb6622
 webpage internal acknowledgement body-background-color #22aa11
 webpage internal acknowledgement body-font-color #bb6622
 webpage internal welcome use-external-success-url
nx9500-6C8809(config-captive-portal-ca-enhanced-policy)#
```

#### Related Commands

|                 |                                                  |
|-----------------|--------------------------------------------------|
| <code>no</code> | Resets or disables captive portal configurations |
|-----------------|--------------------------------------------------|

#### webpage-auto-upload

Enables automatic upload of advanced Web pages to requesting clients on association. Enable this option if the webpage-location is selected as advanced. For more information, see [webpage-location](#).

If this feature is enabled, Access Points shall request for Web pages from the controller during adoption. If the controller has a different set of Web pages, than the ones existing on the Access Points, the controller shall distribute the Web pages uploaded on it to the Access Points.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
webpage-auto-upload
```

#### Parameters

None

#### Examples

```
nx9500-6C8809(config-captive-portal-test)#webpage-auto-upload
nx9500-6C8809(config-captive-portal-test)#show context
captive-portal test
 webpage-auto-upload
 logout-fqdn logout.testuser.com
nx9500-6C8809(config-captive-portal-test)#
```

#### Related Commands

|                               |                                                                       |
|-------------------------------|-----------------------------------------------------------------------|
| <code>no</code>               | Disables automatic upload of advanced Web pages on a captive portal   |
| <code>webpage</code>          | Configures Web pages displayed when interacting with a captive portal |
| <code>webpage-location</code> | Specifies the location of the Web pages used for authentication       |

#### webpage-location

Specifies the location of the Web pages used for authentication. These pages can either be hosted on the system or on an external Web server.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

`webpage-location [advanced|external|internal]`

#### Parameters

`webpage-location [advanced|external|internal]`

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>advanced</code> | Uses Web pages for login, welcome, failure, and terms created and stored on the controller. Select <code>advanced</code> to use a custom-developed directory full of Web page content that can be copied in and out of the controller, service platform, or access point.<br>If selecting <code>advanced</code> , enable the <code>webpage-auto-upload</code> option to automatically launch the advanced pages to requesting clients upon association. For more information, see <a href="#">webpage-auto-upload</a> . |
| <code>external</code> | Uses Web pages for login, welcome, failure, and terms located on an external server. Provide the URL for each of these pages.                                                                                                                                                                                                                                                                                                                                                                                           |
| <code>internal</code> | Uses Web pages for login, welcome, and failure that are automatically generated                                                                                                                                                                                                                                                                                                                                                                                                                                         |

#### Examples

```
nx9500-6C8809(config-captive-portal-test)#webpage-location external
nx9500-6C8809(config-captive-portal-test)#show context
captive-portal test
 access-time 35
 custom-auth info bob bob@examplecompany.com
 connection-mode https
 inactivity-timeout 750
 server host 172.16.10.9
 simultaneous-users 5
 terms-agreement
 webpage-location external
 use aaa-policy test
nx9500-6C8809(config-captive-portal-test)#
```

#### Related Commands

|                                  |                                                                                                                          |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <code>no</code>                  | Resets or disables captive portal Web page settings                                                                      |
| <code>webpage</code>             | Configures a captive portal's Web page (acknowledgment, agreement, login, welcome, fail, no-service, and terms) settings |
| <code>webpage-auto-upload</code> | Enables automatic upload of advanced Web pages on a captive portal                                                       |

#### welcome-back

Enables the provision of direct Internet access to once-registered, captive-portal guest users on subsequent log-ins. When enabled, a registered captive-portal guest user, on subsequent logins, is served the Acknowledgement page only if:

- The `agreement-refresh` option is enabled for device-based (device and device-OTP) registration, and
- The interval between logout and login is lesser than the `agreement-refresh` timeout configured in the WLAN context. If this interval exceeds the `agreement-refresh` timeout, the user is served the

Agreement page. For more information on configuring the agreement-refresh timeout value, see [registration](#).

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

### Syntax

```
welcome-back pass-through
```

### Parameters

```
welcome-back pass-through
```

|                           |                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| welcome-back pass-through | Enables display of the Acknowledgement page to an already registered user on subsequent captive-portal log-ins, provided the interval between logout and login is lesser than the agreement-refresh timeout <ul style="list-style-type: none"><li>• pass-through - Provides user direct Internet access, from the Welcome-back page, without any user action</li></ul> |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config-captive-portal-test)#show context
captive-portal test
 welcome-back pass-through
 webpage internal registration field city type text enable label "City" placeholder "Enter City"
 webpage internal registration field street type text enable label "Address" placeholder "123 Any Street"
 webpage internal registration field name type text enable label "Full Name" placeholder "Enter First Name, Last Name"
 webpage internal registration field zip type number enable label "Zip" placeholder "Zip"
 webpage internal registration field via-sms type checkbox enable title "SMS Preferred"
 webpage internal registration field mobile type number enable label "Mobile" placeholder "Mobile Number with Country code"
 webpage internal registration field age-range type dropdown-menu enable label "Age Range" title "Age Range"
 webpage internal registration field email type e-address enable mandatory label "Email" placeholder "you@domain.com"
 webpage internal registration field via-email type checkbox enable title "Email Preferred"nx9500-6C8809(config-captive-portal-test)#
```

### Related Commands

|    |                                                                                                                       |
|----|-----------------------------------------------------------------------------------------------------------------------|
| no | Disables the provision of direct Internet access to once-registered, captive-portal guest users on subsequent log-ins |
|----|-----------------------------------------------------------------------------------------------------------------------|

no (captive-portal-config-mode)

The no command reverts the selected captive portal's settings or resets settings to default.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
no [access-time|access-type|accounting|bypass|connection-mode|custom-auth|data-limit|
frictionless-onboarding|inactivity-timeout|ipv6|localization|logout-fqdn|oauth|php-helper|
post-authentication-vlan|radius-vlan-assignment|redirection|report-loyalty-application|
server|
simultaneous-users|terms-agreement|use|webpage|webpage-auto-upload|webpage-location|
welcome-back]
no [access-time|access-type|connection-mode|data-limit|frictionless-onboarding|
inactivity-timeout|logout-fqdn|post-authentication-vlan|radius-vlan-assignment|
report-loyalty-application|simultaneous-users|terms-agreement|webpage-auto-upload
|webpage-location]
no accounting [radius|syslog]
no bypass captive-portal-detection
no custom-auth info
no ipv6 server host
no localization [fqdn|response]
no oauth {client-id}
no php-helper
no redirection ports
no server host
no server mode {centralized-controller [hosting-vlan-interface]}
no use [aaa-policy|dns-whitelist]
no webpage external [acknowledgement|agreement|fail|login {post}|no-service|
registration|welcome]
no webpage internal [acknowledgement|agreement|fail|login|no-service|org-name|
org-signature|registration|welcome]
no webpage internal [org-name|org-signature]
no webpage internal [acknowledgment|agreement|fail|login|no-service]
[body-background-color|body-font-color|description|footer|header|main-logo|org-background-
color|
org-font-color|small-logo|title]
no webpage internal registration [body-background-color|body-font-color|description|field|
footer|header|main-logo|org-background-color|org-font-color|small-logo|title]
no webpage internal registration field [age-range|city|country|custom <FIELD-NAME>|
disclaimer|dob|email|gender|member|mobile|name|optout|street|via-email|via-sms|zip]
{enable}
no webpage internal welcome [body-background-color|body-font-color|description|footer|
header|main-logo|org-background-color|org-font-color|small-logo|title|use-external-success-
url]
no welcome-back pass-through
```

## Parameters

```
no <PARAMETERS>
```

|                 |                                                                                   |
|-----------------|-----------------------------------------------------------------------------------|
| no <PARAMETERS> | Removes or resets this captive portal's settings, based on the parameters passed. |
|-----------------|-----------------------------------------------------------------------------------|

## Example

The following example shows the captive portal 'test' settings before the 'no' commands are executed:

```
nx9500-6C8809(config-captive-portal-test)#show context
captive-portal test
 access-type logging
 access-time 35
 custom-auth info bob bob@examplecompany.com
 connection-mode https
 inactivity-timeout 750
```

```

accounting syslog host 172.16.10.13 port 1
nx9500-6C8809(config-captive-portal-test)#
nx9500-6C8809(config-captive-portal-test)#no accounting syslog
nx9500-6C8809(config-captive-portal-test)#no access-type
The following example shows the captive portal 'test' settings after the 'no' commands are
executed:
nx9500-6C8809(config-captive-portal-test)#show context
captive-portal test
 access-time 35
 custom-auth info bob bob@examplecompany.com
 connection-mode https
 inactivity-timeout 750
nx9500-6C8809(config-captive-portal-test)#

```

## configuring-device-registration-with-dynamic-vlan-assignment

This section provides the configurations required to enable device registration with dynamic VLAN assignment in a multi-vendor environment.

- 1 Create vendor-specific RADIUS user groups and assign an allowed VLAN to each group, as shown in the following examples:

```

nx9500-6C8809(config)#radius-group Apple
nx9500-6C8809(config-radius-group-Apple)#policy vlan 200
nx9500-6C8809(config)#radius-group Samsung
nx9500-6C8809(config-radius-group-Samsung)#policy vlan 100
nx9500-6C8809(config)#radius-group Devices
nx9500-6C8809(config-radius-group-Devices)#policy vlan 1

```

### Note



If necessary, configure the session-time for each of the above configured RADIUS group. This is the duration for which a RADIUS group client's session remains active after successful authentication. Upon expiration, the RADIUS session is terminated. Use the **policy > session-time > <5-144000>** command to specify the session-time.

- 2 Create a RADIUS user pool, add users to the pool, and assign the users to the vendor-specific user groups: as shown in the following examples:

```

nx9500-6C8809(config)#radius-user-pool-policy Vendor-Devices
nx9500-6C8809(config-radius-user-pool-Vendor-Devices)#user Samsung password 0 samsung
group Samsung
nx9500-6C8809(config-radius-user-pool-Vendor-Devices)#user test password 0 test123
group Apple

```

- 3 Create a RADIUS server policy, and associate the RADIUS groups and user pool created in steps 1 and 2 respectively, as shown in the following examples:

```

nx9500-6C8809(config)#radius-server-policy Guest-Radius
nx9500-6C8809(config-radius-server-policy-Guest-Radius)#use radius-user-pool-policy
Vendor-Devices
nx9500-6C8809(config-radius-server-policy-Guest-Radius)#use radius-group Samsung
nx9500-6C8809(config-radius-server-policy-Guest-Radius)#use radius-group Sony
nx9500-6C8809(config-radius-server-policy-Guest-Radius)#use radius-group Apple

```

- 4 Create an AAA Policy, on the controller, and configure the authentication server as self, as shown in the following example:

```

nx9500-6C8809(config)#aaa-policy OnBoard-NX
nx9500-6C8809(config-aaa-policy-OnBoard-NX)#authentication server 1 onboard controller
nx9500-6C8809(config-aaa-policy-OnBoard-NX)#show context
aaa-policy OnBoard-NX
 authentication server 1 onboard self
nx9500-6C8809(config-aaa-policy-OnBoard-NX)#

```

- 5 Create a captive-portal, and point to the captive-portal's server, enable RADIUS VLAN assignment, and associate the AAA policy, as shown in the following examples:

```

nx9500-6C8809(config)#captive-portal DeviceRegistration
nx9500-6C8809(config-captive-portal-DeviceRegistration)#server host
captive.extremenoc.com
nx9500-6C8809(config-captive-portal-DeviceRegistration)#radius-vlan-assignment
nx9500-6C8809(config-captive-portal-DeviceRegistration)#use aaa-policy OnBoard-NX
nx9500-6C8809(config-captive-portal-DeviceRegistration)#access-type radius

```

- 6 Configure a WLAN and enable RADIUS VLAN assignment, as shown in the following examples:

```

nx9500-6C8809(config)#wlan CP-OnBoarding
nx9500-6C8809(config-wlan-CP-OnBoarding)#ssid CP-OnBoarding
nx9500-6C8809(config-wlan-CP-OnBoarding)#radius vlan-assignment
nx9500-6C8809(config-wlan-CP-OnBoarding)#use aaa-policy OnBoard-NX
nx9500-6C8809(config-wlan-CP-OnBoarding)#use captive-portal DeviceRegistration
nx9500-6C8809(config-wlan-CP-OnBoarding)#captive-portal-enforcement fall-back
nx9500-6C8809(config-wlan-CP-OnBoarding)#registration device group-name Devices expiry-
time 4320
nx9500-6C8809(config-wlan-CP-OnBoarding)#authentication-type mac

```

- 7 Create an access point profile, associate the RADIUS server policy, captive-portal policy to it, and also assign the WLAN to the AP radio, as shown in the following examples:

```

nx9500-6C8809(config-profile-SITE-10)#use radius-server-policy Guest-Radius
nx9500-6C8809(config-profile-SITE-10)#use captive-portal server DeviceRegistration
nx9500-6C8809(config-profile-SITE-10-if-radio2)#wlan CP-OnBoarding bss 1 primary
nx9500-6C8809(config-profile-SITE-10-if-gel1)#switchport mode trunk
nx9500-6C8809(config-profile-SITE-10-if-gel1)#switchport trunk native vlan 90
nx9500-6C8809(config-profile-SITE-10-if-gel1)#switchport trunk allowed vlan
1,90,1000-1002
nx9500-6C8809(config-profile-SITE-10-if-gel1)#no switchport trunk native tagged

```

- 8 Use the access point profile in the access point's device context.

#### Related Commands

|                                                                |                                                                                                                                                                |
|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">radius-server-policy</a> on page 1559              | Documents RADIUS server policy configuration commands                                                                                                          |
| <a href="#">radius-group</a> on page 1551                      | Documents RADIUS group policy configuration commands                                                                                                           |
| <a href="#">radius-user-pool-policy</a> on page 1576           | Documents RADIUS user policy configuration commands                                                                                                            |
| <a href="#">AAA-POLICY</a> on page 1316                        | Documents AAA policy configuration commands                                                                                                                    |
| <a href="#">captive-portal</a> on page 293                     | Documents captive-portal configuration commands                                                                                                                |
| <a href="#">wlan</a> on page 554                               | Documents WLAN configuration commands                                                                                                                          |
| <a href="#">PROFILES</a> on page 857                           | Documents profile configuration commands                                                                                                                       |
| <a href="#">guest-registration</a> on page 750 (show commands) | Documents <b>show &gt; guest-registration</b> command and outputs. Use this command to view guest registration statistics once device-registration is enabled. |

#### configuring WeChat Wi-Fi hotspot support in WiNG captive portal

WeChat is a popular messaging app used in China with more than 500 million installations. WeChat's WiFi hotspot solution allows businesses to provide Internet access to their customers. The WiNG captive portal can be configured to incorporate the WeChat WiFi hotspot, so that WeChat users, on their first connect to a WiNG access point, can automatically authenticate with the WeChat server through an intermediate server.

This section provides an example that shows the configurations required to be made on the WiNG portal to enable WeChat Wi-Fi hotspot.

- 1 Create an AAA policy re-directing the WiNG captive portal user to WeChat's AAA server for authentication, as shown in the following example:

```
nx9500-6C8809(config)#aaa-policy cloud2
nx9500-6C8809(config-aaa-policy-cloud2)#authentication server 1 host
cloud2.synchroweb.com secret 0 firmware
nx9500-6C8809(config-aaa-policy-cloud2)#show context
aaa-policy cloud2
authentication server 1 host cloud2.synchroweb.com secret 0 firmware
nx9500-6C8809(config-aaa-policy-cloud2)#
```



#### Note

Synchroweb is an ISV (independent software vendor), whose third-party software is being used as the intermediate server. The AAA server and RADIUS accounting server configured in AAA policy must be as per the specification provided by the ISV.

- 2 Create a DNS whitelist, whitelisting WeChat's server name in order to initiate RADIUS authentication. The "qq.com" domain name is where WeChat server can be reached.

```
nx9500-6C8809(config)#dns-whitelist wxWL
nx9500-6C8809(config-dns-whitelist-wxWL)#permit cloud2.synchroweb.com
nx9500-6C8809(config-dns-whitelist-wxWL)#permit qq.com suffix
nx9500-6C8809(config-dns-whitelist-wxWL)#show context
dns-whitelist wxWL
permit qq.com suffix
permit cloud2.synchroweb.com
nx9500-6C8809(config-dns-whitelist-wxWL)#
```

- 3 Create a captive portal and associate the AAA policy and DNS whitelist created in steps 1 & 2, as shown in the following example:

```
nx9500-6C8809(config)#captive-portal wxCP
nx9500-6C8809(config-captive-portal-wxCP)#use aaa-policy cloud2
nx9500-6C8809(config-captive-portal-wxCP)#use dns-whitelist wxWL
```

- 4 Configure the following captive portal parameters:

```
nx9500-6C8809(config)#captive-portal wxCP
nx9500-6C8809(config-captive-portal-wxCP)#access-time 10
nx9500-6C8809(config-captive-portal-wxCP)#server host guest.extreme.com
nx9500-6C8809(config-captive-portal-wxCP)#webpage-location external
nx9500-6C8809(config-captive-portal-wxCP)#webpage external login http://
cloud2.synchroweb.com/wechat.nx/index.phpc=WING_TAG_CLIENT_MAC
nx9500-6C8809(config-captive-portal-wxCP)#show context
captive-portal wxCP
access-time 10
server host guest.extreme.com
webpage-location external
webpage external login http://cloud2.synchroweb.com/wechat.nx/
index.phpc=WING_TAG_CLIENT_MAC
use aaa-policy cloud2
use dns-whitelist wxWL
--More--
nx9500-6C8809(config-captive-portal-wxCP)#
```



#### Note

The login URL configured here must be as per the specifications provided by the ISV.



**Note**

The access-type remains unchanged (i.e. radius, which is the default setting). The access-time is set to a minimum value (10 minutes in this example) in order to avoid the default value of 24 hours being applied, in case the RADIUS response does not contain the session-timeout attribute.

- 5 Create a WLAN and associate the captive portal created in step 3:

```
nx9500-6C8809(config)#wlan wxOpen
nx9500-6C8809(config-wlan-wxOpen)#ssid wxOpen
nx9500-6C8809(config-wlan-wxOpen)#vlan 200
nx9500-6C8809(config-wlan-wxOpen)##use captive-portal wxCP
nx9500-6C8809(config-wlan-wxOpen)#captive-portal-enforcement
nx9500-6C8809(config-wlan-wxOpen)#show context
wlan wxOpen
ssid wxOpen
vlan 200
bridging-mode local
encryption-type none
authentication-type none
use captive-portal wxCP
captive-portal-enforcement
nx9500-6C8809(config-wlan-wxOpen)#
```



**Note**

The modes of authentication and encryption remain unchanged (i.e. none, which is the default setting for both parameters). Ensure captive-portal-enforcement is enabled on the WLAN.

Following are the related commands:

|                                            |                                                      |
|--------------------------------------------|------------------------------------------------------|
| <a href="#">AAA-POLICY</a> on page 1316    | Documents AAA policy configuration mode commands     |
| <a href="#">dns-whitelist</a> on page 374  | Documents DNS whitelist configuration mode commands  |
| <a href="#">captive-portal</a> on page 293 | Documents captive portal configuration mode commands |
| <a href="#">wlan</a> on page 554           | Documents WLAN configuration mode commands           |

configuring ExtremeGuest captive portal

This section documents the basic configurations required to deploy an EGuest (ExtremeGuest) setup. A typical EGuest deployment consists of the EGuest server, EGuest captive-portal database, and NOC adopting the access points. The EGuest server and database can be hosted only on the VX 9000 platform.

In the following example, the EGuest server and database are hosted on the same device.

- 1 On the EGuest server/database host,
  - a enable the EGuest daemon. When enabled, the EGuest server is up and running.  
`EG-Server-DB(config-device-02-EE-1A-7E-AE-5B)#eguest-server`
  - b apply a database-policy to enable the EGuest database.  
`EG-Server-DB(config-device-02-EE-1A-7E-AE-5B)#use database-policy default`
  - c configure the NTP server. This is to ensure time synchronization across replica-set members (this is mandatory in replica-set deployments and should be configured either on the replica-set members' device or profile context).  
`EG-Server-DB(config-device-02-EE-1A-7E-AE-5B)#ntp server time.nist.govt`



## 2 On the NOC,

### a create an AAA policy with the following configurations:

- Configure the EGuest server (configured in Step 1) as the authentication and accounting RADIUS server.

```
NOC(config-aaa-policy-EguestAAA)#authentication server 1 host EG-Server secret 0
extreme123
```

```
NOC(config-aaa-policy-EguestAAA)#accounting server 1 host EG-Server secret 0
extreme123
```

- Configure the proxy-mode as 'through-controller'. When configured, all requests to the server are proxied through the NOC.

```
NOC(config-aaa-policy-EguestAAA)#authentication server 1 proxy-mode through-
controller
```

```
NOC(config-aaa-policy-EguestAAA)#accounting server 1 proxy-mode through-controller
```

```
NOC(config-aaa-policy-EguestAAA)#show context
```

```
aaa-policy EguestAAA
```

```
accounting server 1 host EG-OnBServer secret 0 extreme123
```

```
accounting server 1 proxy-mode through-controller
```

```
authentication server 1 host EG-Server secret 0 extreme123
```

```
authentication server 1 proxy-mode through-controller
```

```
NOC(config-aaa-policy-EguestAAA)#
```

### b Create a DNS whitelist. Note, DNS whitelist configuration is required only if enabling OAuth on the EGuest captive-portal. When created and used on the EGuest captive-portal, the DNS whitelist renders social plugin buttons on the client prior to successful captive portal authentication.

- Configure the following permit rules:

```
NOC(config-dns-whitelist-EguestDNS)#permit fbstatic-a.akamaihd.net
```

```
NOC(config-dns-whitelist-EguestDNS)#permit connect facebook.net
```

```
NOC(config-dns-whitelist-EguestDNS)#permit facebook.com suffix
```

```
NOC(config-dns-whitelist-EguestDNS)#permit fbcdn.net suffix
```

```
NOC(config-dns-whitelist-EguestDNS)#permit googleapis.com suffix
```

```
NOC(config-dns-whitelist-EguestDNS)#permit google.com suffix
```

```
NOC(config-dns-whitelist-EguestDNS)#permit googleusercontent.com suffix
```

```
NOC(config-dns-whitelist-EguestDNS)#permit linkedin.com suffix
```

```
NOC(config-dns-whitelist-EguestDNS)#permit static.licdn.com
```

```
NOC(config-dns-whitelist-EguestDNS)#permit twitter.com suffix
```

```
NOC(config-dns-whitelist-EguestDNS)#permit twimg.com suffix
```

```
NOC(config-dns-whitelist-EguestDNS)#permit instagramstatic-a.akamaihd.net
```

```
NOC(config-dns-whitelist-EguestDNS)#permit instagram.com suffix
```

```
NOC(config-dns-whitelist-EguestDNS)#permit ssl.gstatic.com
```

```
NOC(config-dns-whitelist-EguestDNS)#permit extremenetworks.com suffix
```

```
NOC(config-dns-whitelist-EguestDNS)#permit local.extreme.com
```

### c Create a captive-portal with the following configurations:

- Specify the captive-portal server.

```
NOC(config-captive-portal-EguestCP)#server host guest.extreme.com
```

- Use the AAA policy created in Step 2 a.

```
NOC(config-captive-portal-EguestCP)#use aaa-policy EguestAAA
```

- Enable social-media authentication. This setting is optional.

```
NOC(config-captive-portal-EguestCP)#oauth
```

- Use the DNS whitelist created in Step 2 b. Note, the DNS whitelist is required only if enabling OAuth on the captive-portal.  
`NOC(config-captive-portal-EguestCP)#use dns-whitelist EguestDNS`
- Configure the captive portal's webpage location as advanced.



**Note**

Webpage-location should be 'advanced' if using pages created with EGuest splash templates.

```
NOC(config-captive-portal-EguestCP)#webpage-location advanced
```

d Create a WLAN policy with the following configurations:

- Enable MAC authentication.  
`NOC(config-wlan-EguestWLAN)#authentication-type mac`
- Use the AAA policy created in Step 2 a.  
`NOC(config-wlan-EguestWLAN)#use aaa-policy EguestAAA`



**Note**

When used, access points/controllers forward registration requests to the EGuest server specified in the AAA policy. However, ensure that the **registration > external > follow-aaa** option is configured on the WLAN. See below.

```
NOC(config-wlan-EguestWLAN)#registration external follow-aaa
```



**Note**

This enables the use of the Authentication and Accounting servers specified in the AAA policy applied on the WLAN.

- Use the captive-portal created in Step 2 c.  
`NOC(config-wlan-EguestWLAN)#use captive-portal EguestCP`
- Enable captive-portal enforcement with fall-back.  
`NOC(config-wlan-EguestWLAN)#captive-portal-enforcement fall-back`
- Configure the following guest registration parameters:  
`NOC(config-wlan-EguestWLAN)#registration device group-name Eguest expiry-time 4320 agreement-refresh 1440`



**Note**

This is the RADIUS group assigned to registered users post authentication.

```
NOC(config-wlan-EguestWLAN)#show context
wlan EguestWLAN
ssid _EXTREME-GUEST-NRF2017
vlan 1
bridging-mode local
encryption-type none
authentication-type mac
no answer-broadcast-probes
no client-client-communication
wireless-client hold-time 300
use aaa-policy EguestAAA
use captive-portal EguestCP
captive-portal-enforcement fall-back
registration device group-name Eguest expiry-time 4320 agreement-refresh 1440
registration external follow-aaa
```

```
mac-authentication cached-credentials
NOC(config-wlan-EgustWLAN)#
```

e In the NOC's self context, configure the EGuest server.

```
NOC(config-device-74-67-F7-5C-64-4A)#eguest-server host 1 EG-Server https
```

3 In the Access Point's device or profile context, use the captive-portal configured in Step 2 c.

```
Egust-AP(config-device-74-67-F7-5C-64-4A)#use captive-portal EgustCP
```

4 To view EGuest registration status and statistics, on the EGuest server, use the following commands:

```
EG-Server-DB#show eguest registration statistics
EG-Server-DB#show eguest registration status
```

5 To clear EGuest registration statistics, on the EGuest server, use the following command:

```
EG-Server-DB#clear eguest registration statistics
```

Following are the related commands:

|                                                         |                                                                                                                                                                                                                                           |
|---------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">AAA-POLICY</a> on page 1316                 | Documents AAA policy configuration mode commands                                                                                                                                                                                          |
| <a href="#">dns-whitelist</a> on page 374               | Documents DNS whitelist configuration mode commands                                                                                                                                                                                       |
| <a href="#">captive-portal</a> on page 293              | Documents captive portal configuration mode commands                                                                                                                                                                                      |
| <a href="#">wlan</a> on page 554                        | Documents WLAN configuration mode commands                                                                                                                                                                                                |
| <a href="#">eguest-server (VX9000 only)</a> on page 990 | Documents the eguest-server command. When used in the EGuest server's device/profile context, without the 'host' option, it enables the EGuest daemon. When used on the NOC along with the 'host' option, it points to the EGuest server. |
| <a href="#">eguest</a> on page 732 (show commands)      | Documents the <b>show &gt; eguest</b> command outputs                                                                                                                                                                                     |

## clear

Clears parameters, cache entries, table entries, and other similar entries. The clear command is available for specific commands only. The information cleared using this command varies depending on the mode where executed.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
clear event-history
```

### Parameters

```
clear event-history
```

|               |                               |
|---------------|-------------------------------|
| event-history | Clears the event history file |
|---------------|-------------------------------|

### Examples

```
rfs4000-880DA7(config)#show event-history
EVENT HISTORY REPORT
Generated on '2017-06-09 14:23:31 IST' by 'admin'
```

```
2017-06-09 14:16:28 rfs4000-880DA7 SYSTEM LOGIN Successfully logged in
```

```

user 'admin' with privilege 'superuser' from 'ssh'
2017-06-09 14:06:21 rfs4000-880DA7 DEVICE OFFLINE Device B4-
C7-99-71-17-28(ap8132-711728) is offline, last seen:10 minutes ago on switchport
ap7522-8330A4:ge1
2017-06-09 13:46:15 rfs4000-880DA7 SYSTEM CONFIG_REVISION Configuration revision
updated to 10 from 9
2017-06-09 13:36:12 rfs4000-880DA7 SYSTEM CONFIG_REVISION Configuration revision
updated to 9 from 8
2017-06-09 13:26:09 rfs4000-880DA7 SYSTEM CONFIG_COMMIT Configuration commit
by user 'cfgd' (site apply config diff) from '127.0.0.1'
2017-06-09 13:16:06 rfs4000-880DA7 DEVICE UNADOPTED
Device('ap8132-711728'/'ap81xx'/B4-C7-99-71-17-28) at rf-domain:'TechPubs' unadopted.
Radios: Count=2, Bss: B4-C7-99-78-53-10|B4-C7-99-78-53-70|
2017-06-09 13:10:047 ap8132-711728 SYSTEM WARM_START System Warm Start
Reason : Upgrade done, reloading... (user: system @ rfs4000-880DA7) Timestamp: Nov 04
11:32:27 2016
2017-06-09 13:06:03 rfs4000-880DA7 DEVICE DEVICE_UPGRADE_REBOOT DEVICEUPGRADE: ap81xx
mac B4-C7-99-71-17-28 Device upgrade rebooting

--More--
rfs4000-880DA7(config)#
rfs4000-880DA7(config)#clear event-history
rfs4000-880DA7(config)#show event-history
EVENT HISTORY REPORT
Generated on '2017-06-09 14:27:05 IST' by 'admin'

rfs4000-880DA7(config)#

```

### *client-identity*

With an increase in *Bring Your Own Device* (BYOD) corporate networks, there is a parallel increase in the number of possible attack scenarios within the network. BYOD devices are inherently unsafe, as the organization's security mechanisms do not extend to these personal devices deployed in the corporate wireless network. Organizations can protect their network by limiting how and what these BYODs can access on and through the corporate network.

Device fingerprinting assists administrators by controlling how BYOD devices access a corporate wireless domain.

Device fingerprinting uses DHCP options sent by the client in request or discover packets to derive a unique signature specific to device class. For example, Apple devices have a different signature from Android devices. The signature is used to classify the devices and assign permissions and restrictions on each device class.

Device fingerprinting is a technique of collecting, analyzing, and identifying traffic patterns originating from remote computing devices. When enabled, device fingerprinting helps to identify a wireless client's device type. There are two methods of fingerprinting devices: Active and Passive.

Active fingerprinting is based on the fact that traffic patterns vary with varying device types. It involves the sending of requests (HTTP etc.) to devices (clients) and analyzing their response to determine the device type. For example, an invalid request is sent to a device, and its error response is analyzed to identify the device type. Since active device fingerprinting involves sending of packets, the probability of the network getting flooded is very high, especially when many devices are being fingerprinted simultaneously.

Passive fingerprinting involves monitoring of devices to check for known traffic patterns specific to devices based on the protocol, driver implementation etc. This method accurately classifies a client's

TCP/IP configuration, OS fingerprints, wireless settings etc. No packets are sent to the device. Some of the commonly used protocols for passive device fingerprinting are, TCP, DHCP, HTTP etc. This feature implements DHCP device fingerprinting, which relies on specific information sent by a wireless client when acquiring IP address and other configuration information from a DHCP server. The feature uses the DHCP options sent by the wireless client in the DHCP request or discover packets to derive a unique signature specific to the class of devices. For example, Apple devices have a different signature than Android devices. This unique signature can then be used to classify the devices and assign permissions and restrictions on each device class.

The `client-identity` command enables device fingerprinting. It creates a new client identity and enters its configuration mode. Client identity is a set of unique fingerprints used to identify a class of devices. This information is used to configure permissions and access rules for the identified class of devices in the network.



#### Note

The WING software provides a set of built-in device fingerprints that load by default and identify client device types. Use the `service > show > client-identity-defaults` command to view default client identity fingerprints.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
client-identity <CLIENT-IDENTITY-NAME>
```

#### Parameters

```
client-identity <CLIENT-IDENTITY-NAME>
```

|                                           |                                                                                                                                                                                                                                                             |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| client-identity<br><CLIENT-IDENTITY-NAME> | Creates a new client identity policy and enters its configuration mode <ul style="list-style-type: none"><li>• &lt;CLIENT-IDENTITY-NAME&gt; - Specify a client identity policy name. If the client identity policy does not exist, it is created.</li></ul> |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Usage Guidelines

The following points should be considered when configuring the client identity (device fingerprinting) feature:

- Ensure that DHCP is enforced on the WLANs. For more information on enforcing DHCP on WLANs, see [enforce-dhcp](#).
- Successful identification of different device types depends on the uniqueness of the configured fingerprints. DHCP fingerprinting identifies clients based on the patterns (fingerprints) in the DHCP discover and request messages sent by clients. If different operating systems have the same fingerprints, it will be difficult to identify the device type.
- When associating client identities with a role policy, ensure that the profile/device, under which the role policy is being used, also has an associated client identity group (containing all the client identities used by the role policy).

## Examples

```
rfs4000-229D58(config)#client-identity test
rfs4000-229D58(config-client-identity-test)#?
Client Identity Mode commands:
 dhcp Add a DHCP option based match criteria
 dhcp-match-message-type Specify DHCP message type to match
 no Negate a command or set its defaults

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

rfs4000-229D58(config-client-identity-test)#
```

Use the `service > show > client-identity-defaults` command to view default, built-in, system-provided client identity fingerprints:

```
nx9500-6C8809#service show client-identity-defaults
client-identity Android-2-1
 dhcp 1 message-type request option 55 exact hexstring 0103061c21333a3b79
 dhcp 6 message-type request option 60 exact ascii dhcpcd\ 4.0.1
client-identity Android-2-2
 dhcp 1 message-type request option 55 exact hexstring 01792103061c333a3b
 dhcp 6 message-type request option 60 exact ascii dhcpcd\ 4.0.15
client-identity Android-2-3
 dhcp 3 message-type request option 55 exact hexstring 01792103061c333a3b
 dhcp 6 message-type request option 60 exact ascii dhcpcd\ 4.0.15
 dhcp 1 message-type request option-codes exact hexstring 353d32393c37
 dhcp 2 message-type request option-codes exact hexstring 353d3236393c37
 dhcp 10 message-type request option-codes exact hexstring 353d3236393c0c37
--More--
nx9500-6C8809#
```

## Related Commands

|                                    |                                                |
|------------------------------------|------------------------------------------------|
| <code>no</code>                    | Removes an existing client identity definition |
| <code>client-identity-group</code> | Configures a new client identity group         |

## client-identity-mode-commands

The following table summarizes the client-identity configuration mode commands:

**Table 12: Client-Identity-Mode Commands**

| Command                              | Description                                                             |
|--------------------------------------|-------------------------------------------------------------------------|
| <code>dhcp</code>                    | Configures the DHCP option match criteria for device fingerprinting     |
| <code>dhcp-match-message-type</code> | Configures the DHCP message type for device fingerprinting              |
| <code>no</code>                      | Removes the DHCP option (used for client identification) configurations |

## dhcp

Configures the DHCP option match criteria (signature) for the discover and request message types received from wireless clients

When accessing a network, DHCP discover and request messages are passed between wireless clients and the DHCP server. These messages contain DHCP options and option values that differ from device to device and are based on the DHCP implementation in the device's OS (Operating System). Options and option values contained in a client's messages are parsed and compared against the configured DHCP option values to identify the device. Once a device type is identified, the wireless client database is updated with the discovered device type.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
dhcp <1-16> message-type [discover|request] [option|option-codes]
dhcp <1-16> message-type [discover|request] [option <1-254>|option-codes]
[contains|exact|starts-with] [ascii|hexstring] <WORD>
```

### Parameters

```
dhcp <1-16> message-type [discover|request] [option <1-254>|option-codes]
[contains|exact|starts-with] [ascii|hexstring] <WORD>
```

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dhcp <1-16>                            | <p>Adds a DHCP option match criteria signature</p> <ul style="list-style-type: none"> <li>• &lt;1-16&gt; – Specify an index for this DHCP match criteria from 1 - 16.</li> </ul> <p><b>Note:</b> A maximum of 16 match criteria can be configured.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| message-type<br>[discover]<br>request] | <p>Specifies the message type to which this DHCP match criteria is applicable</p> <ul style="list-style-type: none"> <li>• discover – Applies this match criteria to DHCP discover messages only. Indicates that the fingerprint is only checked with any DHCP discover messages received from any device.</li> <li>• request – Applies this match criteria to DHCP request messages only. Indicates that the fingerprint is only checked with any DHCP request messages received from any device.</li> </ul> <p><b>Note:</b> It is recommended to configure client-identity with request messages, because clients rarely send discover messages.</p> <p><b>Note:</b> If the message type is not specified, the fingerprint is checked with all message types (DHCP request and DHCP discover).</p> |
| option<br><1-254>                      | <p>The following keywords are common to the 'discover' and 'request' message types:</p> <ul style="list-style-type: none"> <li>• option – Configures a DHCP option value, which is used as the match criteria <ul style="list-style-type: none"> <li>• &lt;1-254&gt; – Configures a code for this DHCP option from 1 - 254 (except option 53)</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| option-codes                           | <p>The following keyword is common to the 'discover' and 'request' message types:</p> <ul style="list-style-type: none"> <li>• option-codes – Matches criteria based on the DHCP option codes contained in the client's discover/request messages</li> </ul> <p>Devices pass options in their DHCP discover/request messages as option codes, option types, and option value sets. These option codes are extracted and matched against the configured DHCP option codes and a fingerprint is derived. This derived fingerprint is used to identify the device.</p>                                                                                                                                                                                                                                  |
| contains                               | <p>The following keyword is common to the 'discover' and 'request' message types:</p> <ul style="list-style-type: none"> <li>• contains – Specifies that the DHCP options received in the client's discover/request messages contains the configured option code string</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| exact                                  | <p>The following keyword is common to the discover and request message types:</p> <ul style="list-style-type: none"> <li>• exact – Specifies that the DHCP options received in the client's discover/request messages is an exact match with the configured option code string</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| starts-with                            | <p>The following keyword is common to the 'discover' and 'request' message types:</p> <ul style="list-style-type: none"> <li>• starts-with – Specifies that the DHCP options received in the client's discover/request messages starts with the configured option code string</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| ascii<br><WORD>                        | <p>The following keywords are common to the 'contains', 'exact', and 'starts-with' parameters:</p> <ul style="list-style-type: none"> <li>• ascii – Configures the DHCP option in the ASCII format <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the DHCP option ASCII value to match.</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| hexstring<br><WORD>                    | <p>The following keywords are common to the 'contains', 'exact', and 'starts-with' parameters:</p> <ul style="list-style-type: none"> <li>• hexstring – Configures the DHCP option in the hexa-decimal format <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the DHCP option hexstring value to match.</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

#### Usage Guidelines

The following DHCP options are useful for identifying different device types:



- Option 55: Used by a DHCP client to request values for specific configuration parameters. It is a list of DHCP option codes and can be in the client's order of preference.
- Client configured list of DHCP options (all options parsed into a hex string).
- Option 60: Vendor class identifier. Used to identify the vendor and functionality of a DHCP client (some devices do not set the value of this field).

Though it is possible to use any option to configure a device fingerprint, the use of a combination of one or more of the preceding options to define a device is recommended.

#### Examples

```
rfs4000-229D58(config-client-identity-test)#dhcp 1 message-type request option
60 exact ascii MSFT\5.0
rfs4000-229D58(config-client-identity-test)#dhcp 2 message-type discover option
2 exact hexstring 012456c22c44
rfs4000-229D58(config-client-identity-test)#show context
client-identity test
 dhcp 2 message-type discover option 2 exact hexstring 012456c22c44
 dhcp 1 message-type request option 60 exact ascii MSFT5.0
rfs4000-229D58(config-client-identity-test)#
```

#### Related Commands

|           |                                                  |
|-----------|--------------------------------------------------|
| <b>no</b> | Removes a DHCP option signature (match criteria) |
|-----------|--------------------------------------------------|

#### dhcp-match-message-type

Configures the DHCP message type to match

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
dhcp-match-message-type [all|any|discover|request]
```

#### Parameters

```
dhcp-match-message-type [all|any|discover|request]
```

|                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dhcp-match-message-type [all any discover request] | <p>Specifies the DHCP message type to consider for matching</p> <ul style="list-style-type: none"> <li>• all – Matches all message types: discover and request. Indicates that the fingerprint is checked with both the DHCP request and the DHCP discover message.</li> <li>• any – Matches any message type: discover or request. Indicates that the fingerprint is checked with either the DHCP request or the DHCP discover message.</li> <li>• discover – Matches discover messages only. A match is made only if the discover message sent by the client matches the match criteria set in the client identity. Values configured for request messages are ignored.</li> <li>• request – Matches request messages only. A match is made only if the request message sent by the client matches the match criteria set in the client identity. Values configured for discover messages are ignored.</li> </ul> |
|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
rfs4000-229D58(config-client-identity-test)#dhcp-match-message-type all
rfs4000-229D58(config-client-identity-test)#show context
client-identity test
 dhcp 2 message-type discover option 2 exact hexstring 012456c22c44
 dhcp 1 message-type request option 60 exact ascii MSFT5.0
 dhcp-match-message-type all
rfs4000-229D58(config-client-identity-test)#
```

## Related Commands

|                 |                                        |
|-----------------|----------------------------------------|
| <code>no</code> | Removes the DHCP message type to match |
|-----------------|----------------------------------------|

## no (client-identity-config-mode)

Removes the DHCP options match criteria configurations

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
no [dhcp <1-16>|dhcp-match-message-type]
```

## Parameters

```
no [dhcp <1-16>|dhcp-match-message-type]
```

|                                      |                                                                                                                                                                                                 |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>dhcp &lt;1-16&gt;</code>       | Removes the DHCP option match criteria rule identified by the <1-16> keyword <ul style="list-style-type: none"><li>• &lt;1-16&gt; - Specify the DHCP option match criteria rule index</li></ul> |
| <code>dhcp-match-message-type</code> | Removes the DHCP message type to match                                                                                                                                                          |

## Examples

The following example shows the client identity 'test' settings before the 'no' commands are executed:

```
rfs4000-229D58(config-client-identity-test)#show context
client-identity test
 dhcp 2 message-type discover option 2 exact hexstring 012456c22c44
 dhcp 1 message-type request option 60 exact ascii MSFT5.0
 dhcp-match-message-type all
rfs4000-229D58(config-client-identity-test)#
```

The following example shows the client identity 'test' settings after the 'no' commands are executed:

```
rfs4000-229D58(config-client-identity-test)#no dhcp 2
rfs4000-229D58(config-client-identity-test)#no dhcp-match-message-type
rfs4000-229D58(config-client-identity-test)#show context
client-identity test
 dhcp 1 message-type request option 60 exact ascii MSFT5.0
rfs4000-229D58(config-client-identity-test)#
```

## Related Commands

|                                      |                                                                     |
|--------------------------------------|---------------------------------------------------------------------|
| <code>dhcp</code>                    | Configures the DHCP option match criteria for device fingerprinting |
| <code>dhcp-match-message-type</code> | Configures the DHCP message type for device fingerprinting          |

## *client-identity-group*

Configures a new client identity group

A client identity group is a collection of client identities. Each client identity included in a client identity group is set a priority value that indicates the priority for that identity when device fingerprinting.

Device fingerprinting relies on specific information sent by a wireless client when acquiring IP address and other configuration information from a DHCP server. The feature uses the DHCP options sent by the wireless client in the DHCP request or discover packets to derive a unique signature specific to the class of devices. For example, Apple devices have a different signature than Android devices. This unique signature can then be used to classify the devices and assign permissions and restrictions on each device class.

A client identity group can be attached to a profile or device, enabling device fingerprinting on them.

### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### **Syntax**

```
client-identity-group <CLIENT-IDENTITY-GROUP-NAME>
```

### **Parameters**

```
client-identity-group <CLIENT-IDENTITY-GROUP-NAME>
```

|                                                       |                                                                                                                                                                                                                                                |
|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| client-identity-group<br><CLIENT-IDENTITY-GROUP-NAME> | Creates a new client identity group and enters its configuration mode <ul style="list-style-type: none"><li>• &lt;CLIENT-IDENTITY-GROUP-NAME&gt; - Specify a client identity group name. If the group does not exist, it is created.</li></ul> |
|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### **Examples**

```
rfs4000-229D58(config)#client-identity-group test
rfs4000-229D58(config-client-identity-group-test)#
Client Identity group Mode commands:
 client-identity Client identity (DHCP Device Fingerprinting)
 load Load Client identity Fingerprints
 no Negate a command or set its defaults

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

rfs4000-229D58(config-client-identity-group-test)#
```

## Related Commands

|                 |                                           |
|-----------------|-------------------------------------------|
| <code>no</code> | Removes an existing client identity group |
|-----------------|-------------------------------------------|

## client-identity-group-mode-commands

The following table summarizes the client identity group configuration mode commands:

**Table 13: Client-Identity-Group-Mode Commands**

| Command                                  | Description                                                                                                              |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <code>client-identity</code> on page 344 | Associates an existing and configured client identity (device fingerprinting definition) with this client identity group |
| <code>load</code> on page 345            | Loads default (system-provided) client identity fingerprints                                                             |
| <code>no</code>                          | Removes the client identity associated with this client identity group                                                   |

## client-identity

Associates an existing and configured client identity (device fingerprinting definition) with this client identity group

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
client-identity <CLIENT-IDENTITY-NAME> precedence <1-10000>
```

## Parameters

```
client-identity <CLIENT-IDENTITY-NAME> precedence <1-10000>
```

|                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>client-identity</code><br><code>&lt;CLIENT-IDENTITY-NAME&gt;</code> | Associates a client identity with this group <ul style="list-style-type: none"><li>• <code>&lt;CLIENT-IDENTITY-NAME&gt;</code> – Specify a client identity name (should be existing and configured)</li></ul>                                                                                                                                                                                                                                     |
| <code>precedence</code><br><code>&lt;1-10000&gt;</code>                   | Determines the order in which client identity is used. <ul style="list-style-type: none"><li>• <code>&lt;1-10000&gt;</code> – Specify this client identity precedence from <code>&lt;1-10000&gt;</code>.</li></ul> <p>The client identity rule is applied based on its precedence value. Lower the value, higher is the precedence. Therefore, a client identity with precedence 5 gets priority over a client identity having precedence 20.</p> |

## Examples

The following example shows two client identities created and configured:

```
rfs4000-229D58(config)#show context
!
! Configuration of RFS4000 version 5.9.2.0-006D
!
!
```

```

version 2.5
!
!
client-identity TestClientIdentity
 dhcp 1 message-type request option-codes exact hexstring 5e4d36780b3a7f
!
client-identity test
 dhcp 2 message-type discover option 2 exact hexstring 012456c22c44
 dhcp 1 message-type request option 60 exact ascii MSFT5.0
 dhcp-match-message-type all
!
client-identity-group ClientIdentityGroup
 client-identity TestClientIdentity precedence 1
!
client-identity-group test
!
ip access-list BROADCAST-MULTICAST-CONTROL
 permit tcp any any rule-precedence 10 rule-description "permit all TCP traffic"
 --More--
rfs4000-229D58(config)#

```

The following example associates client identity 'test' with the client identity group 'test':

```
rfs4000-229D58(config-client-identity-group-test)#client-identity test precedence 1
```

The following example shows the client identity group 'test' with two associated client identities having precedence 1 and 2:

```

rfs4000-229D58(config-client-identity-group-test)#client-identity TestClientIdentity
precedence 2
rfs4000-229D58(config-client-identity-group-test)#show context
client-identity-group test
 client-identity test precedence 1
 client-identity TestClientIdentity precedence 2
rfs4000-229D58(config-client-identity-group-test)#

```

#### Related Commands

|                                                                                 |
|---------------------------------------------------------------------------------|
| <b>no</b> Removes the client identity associated with the client identity group |
|---------------------------------------------------------------------------------|

#### load

Loads default (built-in, system-provided) client identity fingerprints. This option is enabled by default.

The WiNG software provides some built-in client identity fingerprints that are automatically loaded when the client identity group is applied to a device (either directly or through the profile).

WiNG, nx9500-6C8809, rfs4000-229D58, rfs4000-1B3596, rfs4000-229D58, nx9500-6C8809, nx9500-6C874D

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
load default-fingerprints
```

#### Parameters

```
load default-fingerprints
```

|                           |                                                                                |
|---------------------------|--------------------------------------------------------------------------------|
| load default-fingerprints | Loads client identity default fingerprints. This option is enabled by default. |
|---------------------------|--------------------------------------------------------------------------------|

## Examples

The auto-load default fingerprints option is enabled by default, as shown in the following example:

```
nx9500-6C874D(config-client-identity-group-test)#show context
client-identity-group test
 load default-fingerprints
nx9500-6C874D(config-client-identity-group-test)#
```

In scenarios where only customized client identities are to be applied, use the **no > load > default-fingerprints** command to disable auto-loading of default device fingerprints.

```
nx9500-6C874D(config-client-identity-group-test)#no load default-fingerprints
nx9500-6C874D(config-client-identity-group-test)#show context
client-identity-group test
 no load default-fingerprints
nx9500-6C874D(config-client-identity-group-test)#
```

Use the **service > show > client-identity-defaults** command to view default client identity fingerprints:

```
nx9500-6C874D#service show client-identity-defaults
client-identity Android-2-1
 dhcp 1 message-type request option 55 exact hexstring 0103061c21333a3b79
 dhcp 6 message-type request option 60 exact ascii dhcpcd\ 4.0.1
client-identity Android-2-2
 dhcp 1 message-type request option 55 exact hexstring 01792103061c333a3b
 dhcp 6 message-type request option 60 exact ascii dhcpcd\ 4.0.15
client-identity Android-2-3
 dhcp 3 message-type request option 55 exact hexstring 01792103061c333a3b
 dhcp 6 message-type request option 60 exact ascii dhcpcd\ 4.0.15
 dhcp 1 message-type request option-codes exact hexstring 353d32393c37
 dhcp 2 message-type request option-codes exact hexstring 353d3236393c37
 dhcp 10 message-type request option-codes exact hexstring 353d3236393c0c37
--More--
nx9500-6C874D#
```

## Related Commands

|    |                                                                    |
|----|--------------------------------------------------------------------|
| no | Disables automatic loading of default client identity fingerprints |
|----|--------------------------------------------------------------------|

no (client-identity-group-config-mode)

Removes the client identity associated with the client identity group

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
no [client-identity|load]
no client-identity <CLIENT-IDENTITY-NAME> precedence <1-10000>
no load default-fingerprints
```

## Parameters

```
no client-identity <CLIENT-IDENTITY-NAME> precedence <1-10000>
```

```
no client-identity <CLIENT-IDENTITY-NAME> precedence <1-10000>
```

Disassociates a specified client identity from this client identity group

- <CLIENT-IDENTITY-NAME> – Specify the client identity name.
- precedence <1-10000> – Specify the above specified client identity's precedence value from <1-10000>.

The client identity rule is applied based on its precedence value. Lower the value, higher is the precedence. Therefore, a client identity with precedence 5 gets precedence over a client identity having precedence 20.

```
no load default-fingerprints
```

```
no load default-fingerprints
```

Disables automatic loading of built-in, system-provided client identity fingerprints

### Examples

```
<exsw5>(config-client-identity-group-test)#show context
client-identity-group test
 client-identity test precedence 1
<exsw5>(config-client-identity-group-test)#
<exsw5>(config-client-identity-group-test)#no client-identity test
<exsw5>(config)#
```

### Related Commands

```
client-identity Associates an existing and configured client identity (device fingerprinting) with this client identity group
```

## clone

Creates a replica of an existing object or device. The configuration of the new object or device is an exact copy of the existing object or device configuration. Use this command to copy existing configurations and then modifying only the required parameters.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
clone [TLO|device]
clone TLO <EXISTING-OBJECT-NAME> <NEW-OBJECT-NAME>
clone device <EXISTING-DEVICE-MAC/NAME> <NEW-DEVICE-MAC>
```

### Parameters

```
clone TLO <EXISTING-OBJECT-NAME> <NEW-OBJECT-NAME>
```

|                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>TLO &lt;EXISTING-OBJECT-NAME&gt;<br/>&lt;NEW-OBJECT-NAME&gt;</p> | <p>Creates a new TLO by cloning an existing top-level object. The new object has the same configuration as the cloned object.</p> <ul style="list-style-type: none"> <li>• &lt;EXISTING-OBJECT-NAME&gt; - Specify the existing object's (to be cloned) name</li> <li>• &lt;NEW-OBJECT-NAME&gt; - Provide the new object's name.</li> </ul> <p><b>Note:</b> Enter <b>clone</b> and press <b>Tab</b> to list objects available for cloning.</p> |
|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

`clone device <EXISTING-DEVICE-MAC/NAME> <NEW-DEVICE-MAC>`

|                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>device &lt;EXISTING-DEVICE-MAC/NAME&gt;<br/>&lt;NEW-DEVICE-MAC&gt;</p> | <p>Configures a new device based on an existing device configuration</p> <ul style="list-style-type: none"> <li>• &lt;EXISTING-DEVICE-MAC/NAME&gt; - Specify the existing device's name or MAC address (the device to be cloned)</li> <li>• &lt;NEW-DEVICE-MAC&gt; - Provide the new device's MAC address.</li> </ul> <p><b>Note:</b> Enter <b>clone &gt; device</b> and press <b>Tab</b> to list devices available for cloning.</p> |
|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Examples**

```

nx9500-6C874D(config)#clone rf_domain TechPubs Cloned_TechPubs2
nx9500-6C874D(config)#show context
!
! Configuration of NX9500 version 5.9.2.0-008B
!
!
version 2.5
!
.....
rf-domain TechPubs
 location SanJose
 timezone America/Los_Angeles
 country-code us
!
rf-domain Cloned_TechPubs2
 location SanJose
--More--
nx9500-6C874D(config)#

```

*crypto-cmp-policy*

Creates a crypto Certificate Management Protocol (CMP) policy and enters its configuration mode

**Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

**Syntax**

`crypto-cmp-policy <CRYPTO-CMP-POLICY-NAME>`

**Parameters**

`crypto-cmp-policy <CRYPTO-CMP-POLICY-NAME>`



```
crypto-cmp-policy <CRYPTO- Specify the crypto CMP policy name. If the policy does not exist, it is created.
CMP-POLICY-NAME>
```

## Examples

```
nx9500-6C8809(config)#crypto-cmp-policy CMP
nx9500-6C8809(config-cmp-policy-CMP)#?
CMP Policy Mode commands:
 ca-server CMP CA Server configuration commands
 cert-key-size Set key size for certificate request
 cert-renewal-timeout Trigger a cert renewal request on timeout
 cross-cert-validate Validate cross-cert using factory-cert
 no Negate a command or set its defaults
 subjectAltName Configure subjectAltName value
 trustpoint Trustpoint for CMP
 use Set setting to use

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-cmp-policy-CMP)#
```

## Related Commands

```
no Resets values or disables commands
```



### Note

For more information on the crypto CMP policy, see [CRYPTO-CMP-POLICY](#) on page 1831.

## customize

Customizes the output of the summary CLI commands. Use this command to define the data displayed as a result of various show commands.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
customize [cdp-lldp-info-column-width|hostname-column-width|show-adoption-status|
show-wireless-client|show-wireless-client-stats|show-wireless-client-stats-rf|
show-wireless-meshpoint|show-wireless-meshpoint-accelerated-multicast|
show-wireless-meshpoint-neighbor-stats|show-wireless-meshpoint-neighbor-stats-rf|
show-wireless-mint-client|show-wireless-mint-client-stats|
show-wireless-mint-client-stats-rf|show-wireless-mint-portal|
```

```

show-wireless-mint-portal-stats|show-wireless-mint-portal-stats-rf|
show-wireless-radio|show-wireless-radio-stats|show-wireless-radio-stats-rf]
customize [cdp-lldp-info-column-width|hostname-column-width] <1-64>
customize show-adoption-status (adopted-by,ap-name <1-64>,cdp-lldp-info,
config-status,last-adoption,msgs,uptime,version)
customize show-wireless-client (ap-name <1-64>,auth,client-identity <1-32>,bss,
enc,hostname <1-64>,ip,last-active,location <1-64>,mac,radio-alias <3-67>,radio-id,
radio-type,role <1-32>,state,username <1-64>,vendor,vlan,wlan)
customize show-wireless-client-stats (hostname <1-64>,mac,rx-bytes,rx-errors,
rx-packets,rx-throughput,t-index,tx-bytes,tx-dropped,tx-packets,tx-throughput)
customize show-wireless-client-stats-rf (average-retry-number,error-rate,
hostname <1-64>,mac,noise,q-index,rx-rate,signal,snr,tx-rate)
customize show-wireless-meshpoint-accelerated-multicast
(ap-hostname,group-addr,mesh-name,neighbor-hostname,neighbor-ifid,radio-alias,
radio-id,radio-mac,subscriptions)
customize show-wireless-meshpoint (ap-mac,cfg-as-root,hops,hostname <1-64>,
interface-ids,is-root,mesh-name <1-64>,mpid,next-hop-hostname <1-64>,next-hop-ifid,
next-hop-use-time,path-metric,root-bound-time,root-hostname <1-64>,root-mpid)
customize show-wireless-meshpoint-neighbor-stats (ap-hostname <1-64>,
neighbor-hostname <1-64>,neighbor-ifid,rx-bytes,rx-errors,rx-packets,rx-throughput,
t-index,tx-bytes,tx-dropped,tx-packets,tx-throughput)
customize show-wireless-meshpoint-neighbor-stats-rf (ap-hostname <1-64>,
average-retry-number,error-rate,neighbor-hostname <1-64>,neighbor-ifid,noise,q-index,
rx-rate,signal,snr,t-index,tx-rate)
customize show-wireless-mint-client (client-alias <1-64>,client-bss,
portal-alias <1-64>,portal-bss,up-time)
customize show-wireless-mint-client-stats (client-alias <1-64>,
portal-alias <1-64>,portal-bss,rx-bytes,rx-errors,rx-packets,rx-throughput,t-index,
tx-bytes,tx-dropped,tx-packets,tx-throughput)
customize show-wireless-mint-client-stats-rf (average-retry-number,
client-alias <1-64>,error-rate,noise,portal-alias <1-64>,portal-bss,q-index,rx-rate,
signal,snr,tx-rate)
customize show-wireless-mint-portal (client-alias <1-64>,client-bss,
portal-alias <1-64>,portal-bss,up-time)
customize show-wireless-mint-portal-stats (client-alias <1-64>,client-bss,
portal-alias <1-64>,rx-bytes,rx-errors,rx-packets,rx-throughput,t-index,tx-bytes,
tx-dropped,tx-packets,tx-throughput)
customize show-wireless-mint-portal-stats-rf (average-retry-number,
client-alias <1-64>,client-bss,error-rate,noise,portal-alias <1-64>,q-index,rx-rate,
signal,snr,tx-rate)
customize show-wireless-radio (adopt-to,ap-name <1-64>,channel,location <1-64>,
num-clients,power,radio-alias <3-67>,radio-id,radio-mac,rf-mode,state)
customize show-wireless-radio-stats (radio-alias <3-67>,radio-id,radio-mac,
rx-bytes,rx-errors,rx-packets,rx-throughput,tx-bytes,tx-dropped,tx-packets,
tx-throughput)
customize show-wireless-radio-stats-rf (average-retry-number,error-rate,
noise,q-index,radio-alias <3-67>,radio-id,radio-mac,rx-rate,signal,snr,t-index,
tx-rate)

```

## Parameters

```
customize [cdp-lldp-info-column-width|hostname-column-width] <1-64>
```

|                                   |                                                                                                                                                                                                                  |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| hostname-column-width <1-64>      | Configures default width of the hostname column in all show commands <ul style="list-style-type: none"> <li>&lt;1-64&gt; - Sets the hostname column width from 1 - 64 characters</li> </ul>                      |
| cdp-lldp-info-column-width <1-64> | Configures the column width in the <b>show &gt; cdp/lldp &gt; [neighbor report]</b> command output <ul style="list-style-type: none"> <li>&lt;1-64&gt; - Sets the column width from 1 - 64 characters</li> </ul> |

```
customize show-adoption-status (adopted-by,ap-name <1-64>,cdp-lldp-info,
config-status,last-adoption,msgs,uptime,version)
```

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show-adoption-status | Configures the information displayed in the show > adoption > status command output. Select the columns (information) displayed from the following options: adopted-by, ap-name, cdp-lldp-info, config-status, last-adoption, msgs, uptime, and version. These are recursive parameters and you can select multiple options at a time. The columns displayed by default are: Device-Name, Version, Config-Status, MSGS, Adopted-By, Last-Adoption, and Uptime. Where ever available, you can optionally use the <1-64> parameter to set the column width. |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
customize show-wireless-client (ap-name <1-64>,auth,client-identity <1-32>,
bss,enc,hostname <1-64>,ip,last-active,location <1-64>,mac,radio-alias <3-67>,
radio-id,radio-type,role <1-32>,state,username <1-64>,vendor,vlan,wlan)
```

|                        |                                                                                                                                                                                                                                                                                                                                        |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show-wireless-client   | Customizes the <b>show &gt; wireless &gt; client</b> command output<br>The columns displayed by default are: MAC, IPv4, Vendor, Radio-ID, WLAN. VLAN, and State.                                                                                                                                                                       |
| ap-name <1-64>         | Includes the ap-name column, which displays the name of the AP with which this client associates <ul style="list-style-type: none"> <li>• &lt;1-64&gt; – Sets the ap-name column width from 1 - 64 characters</li> </ul>                                                                                                               |
| auth                   | Includes the auth column, which displays the authorization protocol used by the wireless client                                                                                                                                                                                                                                        |
| client-identity <1-32> | Includes the client-identity (device type) column, which displays details gathered from DHCP device fingerprinting feature (when enabled). For more information, see <a href="#">client-identity</a> . <ul style="list-style-type: none"> <li>• &lt;1-32&gt; – Sets the client-identity column width from 1 - 32 characters</li> </ul> |
| bss                    | Includes the BSS column, which displays the BSS ID the wireless client is associated with                                                                                                                                                                                                                                              |
| enc                    | Includes the enc column, which displays the encryption suite used by the wireless client                                                                                                                                                                                                                                               |
| hostname <1-64>        | Includes the hostname column, which displays the wireless client's hostname <ul style="list-style-type: none"> <li>• &lt;1-64&gt; – Sets the hostname column width from 1 - 64 characters</li> </ul>                                                                                                                                   |
| ip                     | Includes the IP column, which displays the wireless client's current IP address                                                                                                                                                                                                                                                        |
| last-active            | Includes the last-active column, which displays the time of last activity seen from the wireless client                                                                                                                                                                                                                                |
| location <1-64>        | Includes the location column, which displays the location of the client's associated Access Points <ul style="list-style-type: none"> <li>• &lt;1-64&gt; – Sets the location column width from 1 - 64 characters</li> </ul>                                                                                                            |
| mac                    | Includes the MAC column, which displays the wireless client's MAC address                                                                                                                                                                                                                                                              |
| radio-alias <3-67>     | Includes the radio-alias column, which displays the radio alias with the AP's hostname and radio interface number in the "HOSTNAME:RX" format <ul style="list-style-type: none"> <li>• &lt;3-67&gt; – Sets the radio-alias column width from 3 - 67 characters</li> </ul>                                                              |
| radio-id               | Includes the radio-id column, which displays the radio ID with the AP's MAC address and radio interface number in the "AA-BB-CC-DD-EE-FF:RX" format                                                                                                                                                                                    |
| radio-type             | Includes the radio-type column, which displays the wireless client's radio type                                                                                                                                                                                                                                                        |
| role <1-32>            | Includes the role column, which displays the client's role <ul style="list-style-type: none"> <li>• &lt;1-32&gt; – Sets the role column width from 1 - 32 characters</li> </ul>                                                                                                                                                        |
| state                  | Includes the state column, which displays the wireless client's current availability state                                                                                                                                                                                                                                             |

|                 |                                                                                                                                                                                                          |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| username <1-64> | Includes the username column, which displays the wireless client's username <ul style="list-style-type: none"> <li>• &lt;1-64&gt; – Specify the username column width from 1 - 64 characters.</li> </ul> |
| vendor          | Includes the vendor column, which displays the wireless client's vendor ID                                                                                                                               |
| vlan            | Includes the VLAN column, which displays the wireless client's assigned VLAN                                                                                                                             |
| wlan            | Includes the WLAN column, which displays the wireless client's assigned WLAN                                                                                                                             |

`customize show-wireless-client-stats (hostname <1-64>,mac,rx-bytes,rx-errors,rx-packets,rx-throughput,t-index,tx-bytes,tx-dropped,tx-packets,tx-throughput)`

|                            |                                                                                                                                                                                                              |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show-wireless-client-stats | Customizes the <b>show &gt; wireless &gt; client</b> stats command output<br>The columns displayed by default are: MAC, Tx bytes, RX bytes, Tx pkts, Rx pkts, and Tx bps, RX bps, T-Index, and Dropped pkts. |
| hostname <1-64>            | Includes the hostname column, which displays the wireless client's hostname <ul style="list-style-type: none"> <li>• &lt;1-64&gt; – Sets the hostname column width from 1 - 64 characters</li> </ul>         |
| mac                        | Includes the MAC column, which displays the wireless client's MAC address                                                                                                                                    |
| rx-bytes                   | Includes the rx-bytes column, which displays the total number of bytes received by the wireless client                                                                                                       |
| rx-errors                  | Includes the rx-error column, which displays the total number of errors received by the wireless client                                                                                                      |
| rx-packets                 | Includes the rx-packets column, which displays the total number of packets received by the wireless client                                                                                                   |
| rx-throughput              | Includes the rx-throughput column, which displays the receive throughput at the wireless client                                                                                                              |
| t-index                    | Includes the t-index column, which displays the traffic utilization index at the particular wireless client                                                                                                  |
| tx-bytes                   | Includes the tx-bytes column, which displays the total number of bytes transmitted by the wireless client                                                                                                    |
| tx-dropped                 | Includes the tx-dropped column, which displays the total number of dropped packets by the wireless client                                                                                                    |
| tx-packets                 | Includes the tx-packets column, which displays the total number of packets transmitted by the wireless client                                                                                                |
| tx-throughput              | Includes the tx-throughput column, which displays the transmission throughput at the wireless client                                                                                                         |

`customize show-wireless-client-stats-rf (average-retry-number,error-rate,noise,q-index,rx-rate,signal,snr,t-index,tx-rate)`

|                               |                                                                                                                                                                                                                           |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show-wireless-client-stats-rf | Customizes the <b>show &gt; wireless &gt; client</b> stats RF command output<br>The columns displayed by default are: MAC, Signal (dBm), Noise (dBm), SNR (dB), TX Rate (Mbps), Retry Avg, Errors (pps), and Q-Index (%). |
| average-retry-number          | Includes the average-retry-number column, which displays the average number of retransmissions made per packet                                                                                                            |
| error-rate                    | Includes the error-rate column, which displays the rate of error for the wireless client                                                                                                                                  |
| hostname <1-64>               | Includes the hostname column, which displays the wireless client's hostname <ul style="list-style-type: none"> <li>• &lt;1-64&gt; – Sets the hostname column width from 1 - 64 characters</li> </ul>                      |

|         |                                                                                                                            |
|---------|----------------------------------------------------------------------------------------------------------------------------|
| mac     | Includes the MAC column, which displays the wireless client's MAC address                                                  |
| noise   | Includes the noise column, which displays the noise (in dBm) as detected by the wireless client                            |
| q-index | Includes the q-index column, which displays the RF quality index<br><b>Note:</b> Higher values indicate better RF quality. |
| rx-rate | Includes the rx-rate column, which displays the receive rate at the particular wireless client                             |
| signal  | Includes the signal column, which displays the signal strength (in dBm) at the particular wireless client                  |
| snr     | Includes the snr column, which displays the <i>signal-to-noise</i> (SNR) ratio (in dB) at the particular wireless client   |
| t-index | Includes the t-index column, which displays the traffic utilization index at the particular wireless client                |
| tx-rate | Includes the tx-rate column, which displays the packet transmission rate at the particular wireless client                 |

```
customize show-wireless-meshpoint-accelerated-multicast (ap-hostname,group-addr,
mesh-name,neighbor-hostname,neighbor-ifid,radio-alias,radio-id,radio-mac,subscriptions)
```

|                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show-wireless-meshpoint-accelerated-multicast | Configures the information displayed in the <b>show &gt; wireless &gt; meshpoint &gt; accelerated multicast</b> command output. Select the columns (information) displayed from the following options: ap-hostname, group-addr, mesh-name, neighbor-hostname, neighbor-ifid, radio-alias, radio-id, radio-mac, subscriptions. These are recursive parameters and you can select multiple options at a time.<br><br>The columns displayed by default are: Mesh, Radio, Neighbor-IFID, Neighbor-Hostname, Group-MAC, and Subscriptions. |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
customize show-wireless-meshpoint (ap-mac,cfg-as-root,hops,hostname <1-64>,
interface-ids,is-root,mesh-name <1-64>,mpid,next-hop-hostname <1-64>,next-hop-ifid,
next-hop-use-time,path-metric,root-bound-time,root-hostname <1-64>,root-mpid)
```

|                         |                                                                                                                                                                                                                                                        |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show-wireless-meshpoint | Customizes the <b>show &gt; wireless &gt; meshpoint</b> command output<br>The columns displayed by default are: Mesh, Hostname, Hops, Is-Root, Config-As-Root, Root-Hostname, Root-Bound-Time, Path-Metric, Next-Hop-Hostname, and Next-Hop-Use-Time.  |
| ap-mac                  | Includes the ap-mac column, which displays the AP's MAC address in the AA-BB-CC-DD-EE-FF format. Applicable only in case of non-wireless controller meshpoints                                                                                         |
| cfg-as-root             | Includes the cfg-as-root column, which displays the configured root state of the meshpoint                                                                                                                                                             |
| hops                    | Includes the hops column, which displays the number of hops to the root for this meshpoint                                                                                                                                                             |
| hostname <1-64>         | Includes the hostname column, which displays the AP's hostname. Applicable only in case of non-wireless controller meshpoints <ul style="list-style-type: none"> <li>• &lt;1-64&gt; - Sets the hostname column width from 1 - 64 characters</li> </ul> |
| interface-ids           | Includes the interface-ids column, which displays the interface identifiers (interfaces used by this meshpoint)                                                                                                                                        |
| is-root                 | Includes the is-root column, which displays the current root state of the meshpoint                                                                                                                                                                    |
| mesh-name <1-64>        | Includes the mesh-name column, which displays the meshpoint's name <ul style="list-style-type: none"> <li>• &lt;1-64&gt; - Sets the mesh-name column width from 1 - 64 characters</li> </ul>                                                           |

|                          |                                                                                                                                                                                                                                                            |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mpid                     | Includes the mpid column, which displays the meshpoint identifier in the AA-BB-CC-DD-EE-FF format                                                                                                                                                          |
| next-hop-hostname <1-64> | Includes the next-hop-hostname column, which displays the next-hop AP's name (the AP next in the path to the bound root) <ul style="list-style-type: none"> <li>• &lt;1-64&gt; – Sets the next-hop-hostname column width from 1 - 64 characters</li> </ul> |
| next-hop-ifid            | Includes the next-hop-ifid column, which displays the next-hop interface identifier in the AA-BB-CC-DD-EE-FF format                                                                                                                                        |
| next-hop-use-time        | Includes the next-hop-use-time column, which displays the time since this meshpoint started using this next hop                                                                                                                                            |
| root-bound-time          | Includes the root-bound-time column, which displays the time since this meshpoint has been bound to the current root                                                                                                                                       |
| root-hostname <1-64>     | Includes the root-hostname column, which displays the root AP's hostname to which this meshpoint is bound <ul style="list-style-type: none"> <li>• &lt;1-64&gt; – Sets the root-hostname column width from 1 - 64 characters</li> </ul>                    |
| root-mpid                | Includes the root-mpid column, which displays the bound root meshpoint identifier in the AA-BB-CC-DD-EE-FF format                                                                                                                                          |

customize show-wireless-meshpoint-neighbor-stats (ap-hostname <1-64>, neighbor-hostname <1-64>, neighbor-ifid, rx-bytes, rx-errors, rx-packets, rx-throughput, t-index, tx-bytes, tx-dropped, tx-packets, tx-throughput)

|                                        |                                                                                                                                                                                                                                                               |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show-wireless-meshpoint-neighbor-stats | Customizes the <b>show &gt; wireless &gt; meshpoint &gt; neighbor &gt; stats</b> command output<br>The columns displayed by default are: AP Hostname, Neighbor-IFID, TX bytes, RX bytes, Tx pkts, Rx pkts, Tx (bps), Rx (bps), T-Index (%), and Dropped pkts. |
| ap-name <1-64>                         | Includes the ap-name column, which displays name of the AP reporting a neighbor <ul style="list-style-type: none"> <li>• &lt;1-64&gt; – Sets the ap-name column width from 1 - 64 characters</li> </ul>                                                       |
| neighbor-hostname <1-64>               | Includes the neighbor-hostname column, which displays the reported neighbor's hostname <ul style="list-style-type: none"> <li>• &lt;1-64&gt; – Sets the neighbor-hostname column width from 1 - 64 characters</li> </ul>                                      |
| neighbor-ifid                          | Includes the neighbor-ifid column, which displays the neighbor's interface ID                                                                                                                                                                                 |
| rx-bytes                               | Includes the rx-bytes column, which displays the total bytes received                                                                                                                                                                                         |
| rx-errors                              | Includes the rx-error column, which displays the total bytes of error received                                                                                                                                                                                |
| rx-packets                             | Includes the rx-packets column, which displays the number of packets received                                                                                                                                                                                 |
| rx-throughput                          | Includes the rx-throughput column, which displays neighbor's received throughput                                                                                                                                                                              |
| t-index                                | Includes the t-index column, which displays the traffic utilization index at the neighbor end                                                                                                                                                                 |
| tx-bytes                               | Includes the tx-bytes column, which displays the total bytes transmitted                                                                                                                                                                                      |
| tx-dropped                             | Includes the tx-dropped column, which displays the total bytes dropped                                                                                                                                                                                        |
| tx-packets                             | Includes the tx-packets column, which displays the number of packets transmitted                                                                                                                                                                              |
| tx-throughput                          | Includes the tx-throughput column, which displays neighbor's transmitted throughput                                                                                                                                                                           |

customize show-wireless-meshpoint-neighbor-stats-rf (ap-hostname <1-64>, average-retry-number, error-rate, neighbor-hostname <1-64>, neighbor-ifid, noise, q-index, rx-rate, signal, snr, t-index, tx-rate)

|                                           |                                                                                                                                                                                                                                                                                             |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show-wireless-meshpoint-neighbor-stats-rf | Customizes the <b>show &gt; wireless &gt; meshpoint &gt; neighbor &gt; statistics RF</b> command output<br>The columns displayed by default are: AP Hostname, Neighbor-IFID, Signal (dBm), Noise (dBm), SNR (dB), Tx-Rate (Mbps), Rx-Rate (Mbps), Retry Avg, Errors (pps), and Q-Index (%). |
| ap-name <1-64>                            | Includes the ap-name column, which displays name of the AP reporting a neighbor <ul style="list-style-type: none"> <li>• &lt;1-64&gt; – Sets the ap-name column width from 1 - 64 characters</li> </ul>                                                                                     |
| average-retry-number                      | Includes the average-retry-number column, which displays the average number of retransmissions made per packet.                                                                                                                                                                             |
| error-rate                                | Includes the error-rate column                                                                                                                                                                                                                                                              |
| neighbor-hostname <1-64>                  | Includes the neighbor-hostname, which displays reported neighbor's hostname <ul style="list-style-type: none"> <li>• &lt;1-64&gt; – Sets the neighbor-hostname column width from 1 - 64 characters</li> </ul>                                                                               |
| noise                                     | Includes the noise column, which displays the noise level in dBm                                                                                                                                                                                                                            |
| q-index                                   | Includes the q-index column, which displays the q-index                                                                                                                                                                                                                                     |
| rx-rate                                   | Includes the rx-rate column, which displays rate of receiving                                                                                                                                                                                                                               |
| signal                                    | Includes the signal column, which displays the signal strength in dBm                                                                                                                                                                                                                       |
| snr                                       | Includes the snr column, which displays the signal-to-noise ratio                                                                                                                                                                                                                           |
| t-index                                   | Includes the t-index column, which displays t-index                                                                                                                                                                                                                                         |
| tx-rate                                   | Includes the tx-rate column, which displays rate of transmission                                                                                                                                                                                                                            |

```
customize show-wireless-mint-client (client-alias <1-64>,client-bss,portal-alias <1-64>,portal-bss,up-time)
```

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show-wireless-mint-client | Configures the information displayed in the <b>show &gt; wireless &gt; mint &gt; client</b> command output. Select the columns (information) displayed from the following options: client-alias, client-bss, portal-alias, portal-bss, and up-time. These are recursive parameters and you can select multiple options at a time. The columns displayed by default are: Portal, Portal-Radio-MAC, Client, Client-Radio-MAC, and Up-Time. |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
customize show-wireless-mint-client-stats (client-alias <1-64>,portal-alias <1-64>,portal-bss,rx-bytes,rx-errors,rx-packets,rx-throughput,t-index,tx-bytes,tx-dropped,tx-packets,tx-throughput)
```

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show-wireless-mint-client-stats | Configures the information displayed in the <b>show &gt; wireless &gt; mint &gt; client &gt; statistics</b> command output. Select the columns (information) displayed from the following options: client-alias, portal-alias, portal-bss, rx-bytes, rx-errors, rx-packets, rx-throughput, t-index, tx-bytes, tx-dropped, tx-packets, tx-throughput. These are recursive parameters and you can select multiple options at a time. The columns displayed by default are: Portal, Portal-Radio-MAC, Client, Tx bytes, Rx bytes, TX pkts, Rx pkts, TX (bps), Rx (bps), T-Index (%), and Dropped pkts. Where ever available, you can optionally use the <1-64> parameter to set the column width. |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
customize show-wireless-mint-client-stats-rf (average-retry-number,client-alias <1-64>,error-rate,noise,portal-alias <1-64>,portal-bss,q-index,rx-rate,signal,snr,tx-rate)
```

|                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show-wireless-mint-client-stats-rf | Configures the information displayed in the <b>show &gt; wireless &gt; mint &gt; client &gt; statistics &gt; rf</b> command output. Select the columns (information) displayed from the following options: average-retry-number, client-alias, error-rate, noise, portal-alias, portal-bss, q-index, rx-rate, signal, snr, and tx-rate. These are recursive parameters and you can select multiple options at a time. The columns displayed by default are: MAC, Signal (dBm), Noise (dBm), SNR (dB), Tx-Rate (Mbps), Rx-rate (Mbps), Retry Avg, Errors (pps), and Q-Index (%). Where ever available, you can optionally use the <1-64> parameter to set the column width. |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
customize show-wireless-mint-portal (client-alias <1-64>,client-bss,portal-alias <1-64>,portal-bss,up-time)
```

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show-wireless-mint-portal | Configures the information displayed in the <b>show &gt; wireless &gt; mint &gt; portal</b> command output. Select the columns (information) displayed from the following options: client-alias, client-bss, portal-alias, portal-bss, and up-time. These are recursive parameters and you can select multiple options at a time. The columns displayed by default are: Client, Client-Radio-MAC, Portal, Portal-Radio-MAC, and Up-Time. Where ever available, optionally use the <1-64> parameter to set the column width. |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
customize show-wireless-mint-portal-stats-rf (average-retry-number,client-alias <1-64>,client-bss,error-rate,noise,portal-alias <1-64>,q-index,rx-rate,signal,snr,tx-rate)
```

|                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show-wireless-mint-portal-stats-rf | Configures the information displayed in the <b>show &gt; wireless &gt; mint &gt; portal &gt; statistics &gt; rf</b> command output. Select the columns (information) displayed from the following options: average-retry-number, client-alias, client-bss, error-rate, noise, portal-alias, q-index, rx-rate, signal, snr, tx-rate. These are recursive parameters and you can select multiple options at a time. The columns displayed by default are: Client, Client-Radio-MAC, Portal, Signal (dBm), Noise (dBm), SNR (dB), Tx-Rate (Mbps), Rx-rate (Mbps), Retry Avg, Errors (pps), and Q-Index (%). Where ever available, optionally use the <1-64> parameter to set the column width. |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
customize show-wireless-radio (adopt-to,ap-name <1-64>,channel,location <1-64>,num-clients,power,radio-alias <3-67>,radio-id,radio-mac,rf-mode,state)
```

|                     |                                                                                                                                                                                                                 |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show-wireless-radio | Customizes the show wireless radio command output                                                                                                                                                               |
| adopt-to            | Includes the adopt-to column, which displays information about the wireless controller adopting this AP                                                                                                         |
| ap-name <1-64>      | Includes the ap-name column, which displays information about the AP this radio belongs <ul style="list-style-type: none"> <li>• &lt;1-64&gt; – Sets the ap-name column width from 1 - 64 characters</li> </ul> |
| channel             | Includes the channel column, which displays information about the configured and current channel for this radio                                                                                                 |
| location <1-64>     | Includes the location column, which displays the location of the AP this radio belongs <ul style="list-style-type: none"> <li>• &lt;1-64&gt; – Sets the location column width from 1 - 64 characters</li> </ul> |
| num-clients         | Includes the num-clients column, which displays the number of clients associated with this radio                                                                                                                |
| power               | Includes the power column, which displays the radio's configured and current transmit power                                                                                                                     |





|                    |                                                                                                                                                                                                                                                                                      |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| radio-alias <3-67> | Includes the radio-alias column, which displays the radio's alias (combination of AP's hostname and radio interface number in the "HOSTNAME:RX" formate) <ul style="list-style-type: none"> <li>• &lt;3-67&gt; - Sets the radio-alias column width from 3 - 67 characters</li> </ul> |
| radio-id           | Includes the radio-id column, which displays the radio's ID (combination of AP's MAC address and radio interface number in the "AA-BB-CC-DD-EE-FF:RX" format)                                                                                                                        |
| radio-mac          | Includes the radio-mac column, which displays the radio's base MAC address                                                                                                                                                                                                           |
| rf-mode            | Includes the rf-mode column, which displays the radio's operating mode. The radio mode can be 2.4 GHz, 5.0 GHz, or sensor.                                                                                                                                                           |
| state              | Includes the state column, which displays the radio's current operational state                                                                                                                                                                                                      |

customize show-wireless-radio-stats (radio-alias <3-67>,radio-id,radio-mac,rx-bytes,rx-errors,rx-packets,rx-throughput,tx-bytes,tx-dropped,tx-packets,tx-throughput)

|                           |                                                                                                                                                                                                                                                                                     |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show-wireless-radio-stats | Customizes the show wireless radio statistics command output                                                                                                                                                                                                                        |
| radio-alias <3-67>        | Includes the radio-alias column, which displays the radio's alias (combination of AP's hostname and radio interface number in the "HOSTNAME:RX" format) <ul style="list-style-type: none"> <li>• &lt;3-67&gt; - Sets the radio-alias column width from 3 - 67 characters</li> </ul> |
| radio-id                  | Includes the radio-id column, which displays the radio's ID (combination of AP's MAC address and radio interface number in the "AA-BB-CC-DD-EE-FF:RX" format)                                                                                                                       |
| radio-mac                 | Includes the radio-mac column, which displays the radio's base MAC address                                                                                                                                                                                                          |
| rx-bytes                  | Includes the rx-bytes column, which displays the total number of bytes received by the radio                                                                                                                                                                                        |
| rx-errors                 | Includes the rx-error column, which displays the total number of errors received by the radio                                                                                                                                                                                       |
| rx-packets                | Includes the rx-packets column, which displays the total number of packets received by the radio                                                                                                                                                                                    |
| rx-throughput             | Includes the rx-throughput column, which displays the receive throughput at the radio                                                                                                                                                                                               |
| tx-bytes                  | Includes the tx-bytes column, which displays the total number of bytes transmitted by the radio                                                                                                                                                                                     |
| tx-dropped                | Includes the tx-dropped column, which displays the total number of packets dropped by the radio                                                                                                                                                                                     |
| tx-packets                | Includes the tx-packets column, which displays the total number of packets transmitted by the radio                                                                                                                                                                                 |
| tx-throughput             | Includes the tx-throughput column, which displays the transmission throughput at the radio                                                                                                                                                                                          |

customize show-wireless-radio-stats-rf (average-retry-number,error-rate,noise,-index,radio-alias <3-67>,radio-id,radio-mac,rx-rate,signal,snr,t-index,tx-rate)

|                              |                                                                                                           |
|------------------------------|-----------------------------------------------------------------------------------------------------------|
| show-wireless-radio-stats-rf | Customizes the show wireless radio stats RF command output                                                |
| average-retry-number         | Includes the average-retry-number column, which displays the average number of retransmissions per packet |
| error-rate                   | Includes the error-rate column, which displays the rate of error for the radio                            |

|                    |                                                                                                                                                                                                                                                                                     |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| noise              | Includes the noise column, which displays the noise detected by the radio                                                                                                                                                                                                           |
| q-index            | Includes the q-index column, which displays the RF quality index<br>Higher values indicate better RF quality.                                                                                                                                                                       |
| radio-alias <3-67> | Includes the radio-alias column, which displays the radio's alias (combination of AP's hostname and radio interface number in the "HOSTNAME:RX" format) <ul style="list-style-type: none"> <li>• &lt;3-67&gt; - Sets the radio-alias column width from 3 - 67 characters</li> </ul> |
| radio-id           | Includes the radio-id column, which displays the radio's ID (combination of AP's MAC address and radio interface number in the "AA-BB-CC-DD-EE-FF:RX" format)                                                                                                                       |
| radio-mac          | Includes the radio-mac column, which displays the radio's base MAC address                                                                                                                                                                                                          |
| rx-rate            | Includes the rx-rate column, which displays the receive rate at the particular radio                                                                                                                                                                                                |
| signal             | Includes the signal column, which displays the signal strength at the particular radio                                                                                                                                                                                              |
| snr                | Includes the snr column, which displays the signal-to-noise ratio at the particular radio                                                                                                                                                                                           |
| t-index            | Includes the t-index column, which displays the traffic utilization index at the particular radio                                                                                                                                                                                   |
| tx-rate            | Includes the tx-rate column, which displays the packet transmission rate at the particular radio                                                                                                                                                                                    |

## Examples

The following example shows the shows the show > adoption > status command output before customizing the output:

```
rfs4000-229D58#show adoption status
Adopted by:
Type : nx9000
System Name : nx9500-6C8809
MAC address : B4-C7-99-6C-88-09
MiNT address : 19.6C.88.09
Time : 4 days 22:38:32 ago
```

Adopted Devices:

```

DEVICE-NAME VERSION CFG-STAT MSGS ADOPTED-BY LAST-
ADOPTION UPTIME

ap7532-A2A56C 5.9.2.0-010D configured No rfs4000-229D58 4 days 22:25:56 4 days
22:31:23

```

Total number of devices displayed: 1

```
rfs4000-229D58#
rfs4000-229D58(config)#customize show-adoption-status adopted-by ap-name config-
status last-adoption
rfs4000-229D58(config)#commit
```

The following example shows the shows the show > adoption > status command output after customizing the output:

```
rfs4000-229D58#show adoption status
Adopted by:
Type : nx9000
System Name : nx9500-6C8809
MAC address : B4-C7-99-6C-88-09
MiNT address : 19.6C.88.09
```

```

Time
Adopted Devices:

ADOPTED-BY DEVICE-NAME CFG-STAT LAST-ADOPTION

rfs4000-229D58 ap7532-A2A56C configured 4 days 22:25:56

```

```

Total number of devices displayed: 1
rfs4000-229D58(config)#

```

Use the **no > customize > show-adoption-status** command to revert back to the default format.

```

rfs4000-229D58(config)#no customize show-adoption-status
rfs4000-229D58(config)#commit
rfs4000-229D58#show adoption status
Adopted by:
Type : nx9000
System Name : nx9500-6C8809
MAC address : B4-C7-99-6C-88-09
MiNT address : 19.6C.88.09
Time : 4 days 22:38:32 ago

```

```

Adopted Devices:

DEVICE-NAME VERSION CFG-STAT MSGS ADOPTED-BY LAST-
ADOPTION UPTIME

ap7532-A2A56C 5.9.2.0-010D configured No rfs4000-229D58 4 days 22:25:56 4 days
22:31:23

Total number of devices displayed: 1
rfs4000-229D58#

```

### Related Commands

|                 |                                                       |
|-----------------|-------------------------------------------------------|
| <b>no</b>       | Restores custom CLI settings to default               |
| <b>wireless</b> | Displays wireless configuration and other information |

### *database-client-policy global-config*

Creates a database-client-policy and enters its configuration mode. The database-client-policy configures the IP address or hostname of the database host, and is used on the NSight/EGuest server's device context. However, the database-client-policy is required only in a split deployment, where the server and database are hosted on separate boxes. In such a scenario, the database-client-policy enables the server to identify the database host.

If enforcing database authentication, configure the user-name and password required to access the database on the database-client-policy. For more information on enabling database authentication, see [database \(user and privi exec modes\)](#) on page 59 (user/privi executable mode).

### Supported in the following platforms:

- Service Platforms — NX 95XX, NX 96XX, VX 9000

## Syntax

```
database-client-policy <DATABASE-CLIENT-POLICY-NAME>
```

## Parameters

```
database-client-policy <DATABASE-CLIENT-POLICY-NAME>
```

|                                                             |                                                                                                                                                                                        |
|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| database-client-policy<br><DATABASE-CLIENT-POLICY-<br>NAME> | Specify the database-client-policy name. If the policy does not exist, it is created.<br>Once created and configured, use this policy in the NSight/EGuest server's device<br>context. |
|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
vx9000-34B78B(config)#database-client-policy DBClientPolicy
vx9000-34B78B(config-database-client-policy-DBClientPolicy)#?
```

Database Client Policy Mode commands:

```
authentication Database authentication
database-server Add database server
no Negate a command or set its defaults

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal
```

```
vx9000-34B78B(config-database-client-policy-DBClientPolicy)#
```

To setup a database/server environment, with the database and the server hosted n separate hosts:

- 1 On the database host, use the database policy. This brings up the database server.
- 2 On the NSight/EGuest server, create the database-client-policy, and configure the database host's IP address or hostname.

```
vx9000-34B78B(config)#database-client-policy DBClientPolicy
vx9000-34B78B(config-database-client-policy-DBClientPolicy)#database-server
192.168.13.10
vx9000-34B78B(config-database-client-policy-DBClientPolicy)#show context
database-client-policy DBClientPolicy
database-server 192.168.13.10
vx9000-34B78B(config-database-client-policy-DBClientPolicy)#
```

- 3 Use this database-client-policy in the NSight/EGuest server's device configuration context. Once applied, the server posts details to the database specified in the policy.

```
vx9000-34B78B(config-device-00-0C-29-34-B7-8B)#use database-client-policy DBClientPolicy
vx9000-34B78B(config-device-00-0C-29-34-B7-8B)#show context include-factory | include
database-client-policy
use database-client-policy DBClientPolicy
vx9000-34B78B(config-device-00-0C-29-34-B7-8B)#
```

## Related Commands

|                                                              |                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>no (global-config-mode)</code> on page 475             | Removes an existing database-client-policy                                                                                                                                                                                                                                                                                                         |
| <code>database-policy global config</code> on page 363       | Documents database policy configuration commands. If enforcing authenticated database access, use this command to enable authentication on the database and configure the username and password.                                                                                                                                                   |
| <code>nsight-policy (global-config-mode)</code> on page 479  | Documents NSight policy configuration commands. The NSight policy is a tool, which when created and applied at the RF Domain level allows the RF Domain manager to send statistics (polled from devices within the RF Domain) to the NOC. The NOC, when enabled as the NSight server, stores this data in a locally or externally hosted database. |
| <code>use</code> on page 1232                                | Uses a database-client-policy in the VX 9000's device or profile context                                                                                                                                                                                                                                                                           |
| <code>database (user and privi exec modes)</code> on page 59 | Drops or repairs a database. Also provides database keyfile management capabilities. If enforcing authenticated access to the database, use this command to generate, export, import, and zeroize the keyfile.                                                                                                                                     |

## database-client-policy-commands

The following table summarizes database-client-policy configuration mode commands:

**Table 14: Database Client Policy Config Commands**

| Command                      | Description                                                                                                                                     |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>authentication</code>  | Configures the captive-portal/NSight database users                                                                                             |
| <code>database-server</code> | Configures the database host's IP address or hostname. Use this command to configure the IP address or hostname of the VM hosting the database. |
| <code>no</code>              | Removes the database host's IP/hostname configuration                                                                                           |

### authentication

Configures the database's user account details (username and password)

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 96XX, VX 9000

#### Syntax

```
authentication username <USER-NAME> password <PASSWORD>
```

#### Parameters

```
authentication username <USER-NAME> password <PASSWORD>
```

```
authentication
username <USER-
NAME> password
<PASSWORD>
```

Configures the username and password required to access the database. Note, username and password specified here should be the same as those already created on the database host. For more information on creating database users, see [service](#) on page 647 (common commands).

- username <USER-NAME> - Configures the user name
  - password <PASSWORD> - Configures the password for the username specified above.

However, ensure database authentication is enabled in the database-policy.

**Note:** For more information on database-policy, see [database-policy global config](#) on page 363.

**Note:** For more information on enabling database authentication, see [database \(user and privi exec modes\)](#) on page 59.

### Examples

```
vx9000-65672(config-database-client-policy-DBClientPolicy)# authentication username
extreme password 2 test@12345
vx9000-656725#show running-config database-client-policy replica-set
database-client-policy replica-set
 database-server 13.13.13.3
 database-server 14.14.14.2
 authentication username extreme password 2 q4cUyedmA4BFsn1kg/
xjCQAAAAlIMbdrXKblQbsyrwMGdVzv
vx9000-656725#
```

### Related Commands

|                    |                                                    |
|--------------------|----------------------------------------------------|
| <a href="#">no</a> | Removes an existing database username and password |
|--------------------|----------------------------------------------------|

### database-server

Configures the IPv4/IPv6 address or hostname of the VM hosting the database

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 96XX, VX 9000

### Syntax

```
database-server [<IP> | <HOSTNAME> | <IPv6>]
```

### Parameters

```
database-server [<IP> | <HOSTNAME> | <IPv6>]
```

|                                                |                                                                                                                                                                                                                                                                                          |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| database-server [ <IP>   <HOSTNAME>   <IPv6> ] | Identifies the database host using one of the following options: <ul style="list-style-type: none"><li>• &lt;IP&gt; - Specifies the host's IPv4 address</li><li>• &lt;HOSTNAME&gt; - Specifies the host's hostname</li><li>• &lt;IPv6&gt; - Specifies the host's IPv6 address.</li></ul> |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
vx9000-34B78B(config-database-client-policy-DBClientPolicy)#database-server 192.168.13.10
vx9000-34B78B(config-database-client-policy-DBClientPolicy)#show context
database-client-policy DBClientPolicy
database-server 192.168.13.10
vx9000-34B78B(config-database-client-policy-DBClientPolicy)#
```

### Related Commands

|    |                                                                                       |
|----|---------------------------------------------------------------------------------------|
| no | Removes the database server's (the VM hosting the database) IP/hostname configuration |
|----|---------------------------------------------------------------------------------------|

no (database-client-policy-config-mode)

Removes the database host's IP/hostname configuration. Also removes database user details.

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 96XX, VX 9000

#### Syntax

```
no [authentication|database-server]
no authentication username <USER-NAME>
no database-server [<IP>|<HOST-NAME>|<IPv6>]
```

#### Parameters

```
no [authentication|database-server]
```

|                 |                                                                                                                                          |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------|
| no <PARAMETERS> | Removes the database VM's IPv4/IPv6 address or hostname associated with this database client policy. Also removes database user details. |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
vx9000-34B78B(config-database-client-policy-DBClientPolicy)#show context
database-client-policy DBClientPolicy
database-server 192.168.13.10
vx9000-34B78B(config-database-client-policy-DBClientPolicy)#
vx9000-34B78B(config-database-client-policy-DBClientPolicy)#no database-server
vx9000-34B78B(config-database-client-policy-DBClientPolicy)#show context
database-client-policy DBClientPolicy
vx9000-34B78B(config-database-client-policy-DBClientPolicy)#
```

### *database-policy global config*

Creates a database-policy and enters its configuration mode. After creating the database-policy, use it on the database host. This enables the database. If deploying a database replica-set, use this command to define the replica set configurations.

To enforce database authentication, enable authentication on the database-policy, and configure the username and password required to access the database. Note, this command is part of a set of configurations that are required to enable authentication. For more information on the entire set of configurations, see [database](#) (user exec mode).

#### **Supported in the following platforms:**

- Service Platforms — NX 95XX, NX 96XX, VX 9000

#### **Syntax**

```
database-policy <DATABASE-POLICY-NAME>
```

#### **Parameters**

```
database-policy <DATABASE-POLICY-NAME>
```

|                                        |                                                                                |
|----------------------------------------|--------------------------------------------------------------------------------|
| database-policy <DATABASE-POLICY-NAME> | Specify the database policy name. If the policy does not exist, it is created. |
|----------------------------------------|--------------------------------------------------------------------------------|

## Examples

```
nx9500-6C874D(config)#database-policy test
nx9500-6C874D(config-database-policy-test)#?
Database Policy Mode commands:
 authentication Database authentication
 no Negate a command or set its defaults
 replica-set Replica Set
 shutdown Disable database server

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal
nx9500-6C874D(config-database-policy-test)#
```

## Related Commands

|  |
|--|
|  |
|  |

## database-policy-config-commands

The following table summarizes database-policy configuration mode commands:

**Table 15: Database Policy Config Commands**

| Command                                    | Description                                                                                              |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------|
| <a href="#">authentication</a> on page 364 | Enables database authentication and configures the username and password required to access the database |
| <a href="#">replica-set</a> on page 365    | Adds a member to a database replica set                                                                  |
| <a href="#">shutdown</a> on page 366       | Shuts down the database server                                                                           |
| <a href="#">no</a>                         | Removes a member from the database replica set                                                           |

### authentication

Enables database authentication. When enabled and applied on the database host, this policy enforces authenticated access to the database. This command also configures the username and password required to access the database.

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 96XX, VX 9000

#### Syntax

```
authentication
authentication username <USER-NAME> password <PASSWORD>
```

#### Parameters

```
authentication
```



|                |                                                                                                                                                                                                                                                                                                                       |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| authentication | Enables database authentication on this database-policy. When executed without the associated keywords, the command enables authentication on the database host using the policy. Execute the command along with the username and password inputs to configure the user credentials required for access the database. |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
authentication username <USER-NAME> password <PASSWORD>
```

|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| authentication username <USER-NAME> password <PASSWORD> | <p>Configures the username and password required to access the database. Note, username and password specified here should be the same as those already created on the database host. For more information, see <a href="#">service</a> (common commands).</p> <ul style="list-style-type: none"> <li>username &lt;USER-NAME&gt; - Configures the database username</li> <li>password &lt;PASSWORD&gt; - Configures the password for the username specified above</li> </ul> <p>Users using these credentials are allowed database access. In case of a split NSight/EGuest deployment, ensure that the database-client-policy running on the NSight/EGuest server has the same user details configured. For information on creating database-client-policy, see <a href="#">database-client-policy</a>. For more information on enabling database authentication, see <a href="#">database</a> (user exec mode).</p> |
|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C874D(config-database-policy-test)#authentication
nx9500-6C874D(config-database-policy-test)#no shutdown
nx9500-6C874D(config-database-policy-test)#authentication username user1 password uesr@123
nx9500-6C874D(config-database-policy-test)#show context
database-policy test
 authentication
 authentication username user1 password 2 f20/dTjYiMnR/tqbGFaO5gAAAAjL/xo8clisk1TZjimo128t
nx9500-6C874D(config-database-policy-test)#
```

#### Related Commands

|    |                                                                                        |
|----|----------------------------------------------------------------------------------------|
| no | Disables database authentication, and removes the username and password configuration. |
|----|----------------------------------------------------------------------------------------|

#### replica-set

Adds a member to a database replica set. A replica-set is a group of devices (replica-set members) running the database instances that maintain the same data set. Replica sets provide redundancy and high availability and are the basis for all production deployments. The replica set usually consists of: an arbiter, a primary member, and one or more secondary members. The primary member and the secondary member(s) maintain replicas of the data set.

Before deploying a replica set, ensure that each of the replica-set member:

- has the DB instances installed, and
- is able to communicate with every other member in the set.

After ensuring the above,

- Create a database policy (with identical replica-set configuration) on each of the member devices, and
- Use the database policy in the member device's configuration mode.

These member devices elect a primary member, which begins accepting client-write operations. Remaining devices in the replica-set, with the exception of the arbiter, are designated as secondary members.

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 96XX, VX 9000

#### Syntax

```
replica-set member [<IP>|<FQDN>] {arbiter|priority <0-255>}
```

#### Parameters

```
replica-set member [<IP>|<FQDN>] {arbiter|priority <0-255>}
```

|                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>replica-set member [&lt;IP&gt; &lt;FQDN&gt;] {arbiter priority &lt;0-255&gt;}</pre> | <p>Adds a member to the database replica set. To identify the member, use one of the following options:</p> <ul style="list-style-type: none"><li>• &lt;IP&gt; – Specify the member’s IP address.</li><li>• &lt;FQDN&gt; – Specify the member’s FQDN.</li></ul> <p>After specifying the IP address or FQDN, specify the following:</p> <ul style="list-style-type: none"><li>• arbiter – Optional. Select to configure the member as the arbiter.</li><li>• priority &lt;0-255&gt; – Optional. Configures the priority of a non-arbiter member of the replica set<ul style="list-style-type: none"><li>• &lt;0-255&gt; – Specify the priority from 0 - 255. This value determines the member’s position within the replica set as primary or secondary. It also helps in electing the fall-back primary member in the eventuality of the current primary member being unreachable.</li></ul></li></ul> <p>A replica set should have at least three members. The maximum number of members can go up to fifty (50). However, configuring a three-member replica set is recommended. Replica sets should have odd number of members. In case of an even-numbered replica set, add an arbiter to make the member count odd. This ensures that at least one member gets a majority vote in the primary-member election.</p> |
|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C874D(config-database-policy-test)#replica-set member 192.168.13.14 arbiter
nx9500-6C874D(config-database-policy-test)#replica-set member 192.168.13.16 priority 1
nx9500-6C874D(config-database-policy-test)#replica-set member 192.168.13.12 priority 2
nx9500-6C874D(config-database-policy-test)#show context
database-policy test
 replica-set member 192.168.13.12 priority 2
 replica-set member 192.168.13.14 arbiter
 replica-set member 192.168.13.16 priority 1
nx9500-6C874D(config-database-policy-test)#
```

#### Related Commands

|           |                                                |
|-----------|------------------------------------------------|
| <b>no</b> | Removes a member from the database replica set |
|-----------|------------------------------------------------|

#### shutdown

Shuts down the database server. The factory default is set as **no > shutdown**.

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 96XX, VX 9000

#### Syntax

```
shutdown
```

## Parameters

None

## Examples

```
nx9500-6C874D(config-database-policy-test)#shutdown
nx9500-6C874D(config-database-policy-test)#show context
database-policy test
 shutdown
nx9500-6C874D(config-database-policy-test)#
```

## Related Commands

|                 |                                         |
|-----------------|-----------------------------------------|
| <code>no</code> | Enables (brings-up) the database server |
|-----------------|-----------------------------------------|

no (database-policy-config-mode)

Removes or reverts the database policy settings to default values

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 96XX, VX 9000

## Syntax

```
no [authentication|replica-set|shutdown]
no authentication {username <USER-NAME>}
no replica-set member [<IP>|<FQDN>]
no shutdown
```

## Parameters

no <PARAMETERS>

|                 |                                                                                                                                                     |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| no <PARAMETERS> | Removes a member from the database replica set, or brings up a database server that is down. Also disables database authentication and removes user |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

The following example shows a three-member replica set:

```
nx9500-6C8809(config-database-policy-test)#show context
database-policy test
 replica-set member 192.168.13.12 priority 2
 replica-set member 192.168.13.14 arbiter
 replica-set member 192.168.13.16 priority 1
nx9500-6C8809(config-database-policy-test)#
```

In the following example the arbiter is being removed, leaving the replica set with only two members:

```
nx9500-6C8809(config-database-policy-test)#no replica-set member 192.168.13.14
nx9500-6C8809(config-database-policy-test)#show context
database-policy test
 replica-set member 192.168.13.12 priority 2
 replica-set member 192.168.13.16 priority 1
nx9500-6C8809(config-database-policy-test)#
```

Since a replica set must have at least three members, another member must be added to this replica set. This member may or may not be an arbiter.

```
nx9500-6C8809(config-database-policy-test)#replica-set member 192.168.13.8 priority 3
nx9500-6C8809(config-database-policy-test)#show context
database-policy test
 replica-set member 192.168.13.12 priority 2
 replica-set member 192.168.13.16 priority 1
```

```

 replica-set member 192.168.13.8 priority 3
 nx9500-6C8809(config-database-policy-test)#

```

## device

Enables simultaneous configuration of multiple devices

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```

device {containing/filter}
device {containing <STRING>} {filter type [ap6522/ap6562/ap71xx/ap7502/ap7522/ap7532/ap7562/ap7602/ap7612/ap7622/ap7632/ap7662/ap81xx/ap8432/ap8533/ex3524/ex3548/rfs4000/nx5500/nx75xx/nx9000/nx9600/t5/vx9000]}
device {filter type [ap6522/ap6562/ap71xx/ap7502/ap7522/ap7532/ap7562/ap7602/ap7612/ap7622/ap7632/ap7662/ap81xx/ap8432/ap8533/ex3524/ex3548/rfs4000/nx5500/nx75xx/nx9000/nx9600/t5/vx9000]}

```

### Parameters

```

device {containing <STRING>} {filter type [ap6522/ap6562/ap71xx/ap7502/ap7522/ap7532/ap7562/ap7602/ap7612/ap7622/ap7632/ap7662/ap81xx/ap8432/ap8533/ex3524/ex3548/rfs4000/nx5500/nx75xx/nx9000/nx9600/t5/vx9000]}

```

|                           |                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| device                    | Enters a device's configuration mode. Use this command to simultaneously configure devices having similar configuration.                                                                                                                                                                                                                                |
| containing <STRING>       | Optional. Configures the string to search for in the device's hostname. All devices having hostnames containing the string specified here are filtered, and can be configured simultaneously. <ul style="list-style-type: none"> <li>• &lt;STRING&gt; - Specify the string to search for in the device's hostname.</li> </ul>                           |
| filter type <DEVICE-TYPE> | Optional. Filters out a specific device type. After specifying the hostname string, select the device type. The options are: AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533 EX3524, EX3548, RFS 4000, NX 5500, NX 7510, NX 95XX, NX 96XX, t5 and VX 9000(V-WLC). |

```

device {filter type [ap6522/ap6562/ap71xx/ap7502/ap7522/ap7532/ap7562/ap7602/ap7612/ap7622/ap7632/ap7662/ap81xx/ap8432/ap8533/ex3524/ex3548/rfs4000/nx5500/nx75xx/nx9000/nx9600/t5/vx9000]}

```

|                           |                                                                                                                                                                                                                                                                                           |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| device                    | Configures a basic device profile                                                                                                                                                                                                                                                         |
| filter type <DEVICE-TYPE> | Optional. Filters out a specific device type. The options are: AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533 EX3524, EX3548, RFS 4000, NX 5500, NX 7510, NX 95XX, NX 96XX, t5 and VX 9000(V-WLC). |

### Examples

```

nx9500-6C874D(config)#device filter type ap7532
nx9500-6C874D(config-device-{'type': 'ap7532'})#

```

## Related Commands

|                 |                                           |
|-----------------|-------------------------------------------|
| <code>no</code> | Removes multiple devices from the network |
|-----------------|-------------------------------------------|

### *device-categorization*

Configures a device categorization list, which categorizes devices as sanctioned or neighboring. Categorization of devices enables quick identification and blocking of unsanctioned devices in the network.

Proper classification and categorization of devices (Access Points, clients etc.) helps suppress unnecessary unauthorized Access Point alarms, allowing network administrators to focus on alarms on devices actually behaving in a suspicious manner. An intruder with a device erroneously authorized could potentially perform activities that harm your organization.

Authorized Access Points and clients are generally known to you and conform with your organization's security policies. Unauthorized devices are those detected as interoperating within the network, but are not approved. These devices should be filtered to avoid jeopardizing the data within a managed network. Use this command to apply the neighboring and sanctioned (approved) filters on peer devices operating within a wireless controller or Access Point's radio coverage area. Detected client MAC addresses can also be filtered based on their classification.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
device-categorization <DEVICE-CATEGORIZATION-LIST-NAME>
```

### Parameters

```
device-categorization <DEVICE-CATEGORIZATION-LIST-NAME>
```

|                                   |                                                                                                          |
|-----------------------------------|----------------------------------------------------------------------------------------------------------|
| <DEVICE-CATEGORIZATION-LIST-NAME> | Specify the device categorization list name. If a list with the same name does not exist, it is created. |
|-----------------------------------|----------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config)#device-categorization rfs4000
nx9500-6C8809(config-device-categorization-rfs4000)#?
Device Category Mode commands:
 mark-device Add a device
 no Negate a command or set its defaults

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
```

```

write Write running configuration to memory or terminal
nx9500-6C8809(config-device-categorization-rfs4000)#

```

### Related Commands

|    |                                                |
|----|------------------------------------------------|
| no | Removes an existing device categorization list |
|----|------------------------------------------------|

### device-categorization-mode-commands

The following table summarizes device categorization configuration mode commands:

**Table 16: Device-Categorization Config Mode Commands**

| Command     | Description                                          |
|-------------|------------------------------------------------------|
| mark-device | Adds a device to the device categorization list      |
| no          | Removes a device from the device categorization list |

#### mark-device

Adds a device to the device categorization list as sanctioned or neighboring. Devices are further classified as AP or client.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```

mark-device <1-1000> [sanctioned|neighboring] [ap|client]
mark-device <1-1000> [sanctioned|neighboring] ap {mac <MAC>/ssid <SSID> {mac <MAC>}}
mark-device <1-1000> [sanctioned|neighboring] client {mac <MAC>}

```

#### Parameters

```

mark-device <1-1000> [sanctioned|neighboring] ap {mac <MAC>/ssid <SSID> {mac <MAC>}}

```

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-1000>                   | Configures the device categorization entry index number                                                                                                                                                                                                                                                                                                                                                                                                             |
| sanctioned                 | Marks a device as sanctioned. A sanctioned device is authorized to use network resources.                                                                                                                                                                                                                                                                                                                                                                           |
| neighboring                | Marks a device as neighboring. A neighboring device is a neighbor in the same network as this device.                                                                                                                                                                                                                                                                                                                                                               |
| ap {mac <MAC> ssid <SSID>} | <p>Marks a specified AP as sanctioned or neighboring based on its MAC address or the SSID it is beaconing</p> <ul style="list-style-type: none"> <li>• mac &lt;MAC&gt; – Optional. Specify the AP's MAC address</li> <li>• ssid &lt;SSID&gt; – Optional. Specify the SSID the AP is beaconing. After specifying the SSID, you can optionally specify MAC address of the radio.</li> </ul> <p>All APs are marked if no specific MAC address or SSID is provided.</p> |

```

mark-device [sanctioned|neighboring] client {mac <MAC>}

```

|                    |                                                                                                                                                                                                                  |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-1000>           | Configures the device categorization entry index number                                                                                                                                                          |
| sanctioned         | Marks the wireless client as sanctioned. A sanctioned device is authorized to use network resources.                                                                                                             |
| neighboring        | Marks the wireless client as neighboring. A neighboring device is a neighbor in the same network as this device.                                                                                                 |
| client {mac <MAC>} | Marks a specified wireless client as sanctioned or neighboring based on its MAC address <ul style="list-style-type: none"> <li>mac &lt;MAC&gt; - Optional. Specify the wireless client's MAC address.</li> </ul> |

#### Examples

```

nx9500-6C8809(config-device-categorization-rfs4000)#mark-device 1 sanctioned ap
 mac 11-22-33-44-55-66
nx9500-6C8809(config-device-categorization-rfs4000)#show context
device-categorization rfs4000
 mark-device 1 sanctioned ap mac 11-22-33-44-55-66
nx9500-6C8809(config-device-categorization-rfs4000)#

```

#### Related Commands

|    |                                                      |
|----|------------------------------------------------------|
| no | Removes an entry from the device categorization list |
|----|------------------------------------------------------|

no (device-categorization-config-mode)

Removes a device from the device categorization list

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```

no mark-device <1-1000> [neighboring|sanctioned] [ap|client]
no mark-device <1-1000> [sanctioned|neighboring] client {mac <MAC>}
no mark-device <1-1000> [sanctioned|neighboring] ap {mac <MAC>/ssid <SSID> {mac <MAC>}}

```

#### Parameters

no <PARAMETERS>

|                 |                                                                                          |
|-----------------|------------------------------------------------------------------------------------------|
| no <PARAMETERS> | Removes a mark device (AP or wireless client) entry from this device categorization list |
|-----------------|------------------------------------------------------------------------------------------|

#### Examples

The following example shows the device categorization list 'rfs7000' settings before the 'no' command is executed:

```

nx9500-6C8809(config-device-categorization-rfs4000)#show context
device-categorization rfs4000
 mark-device 1 sanctioned ap mac 11-22-33-44-55-66
nx9500-6C8809(config-device-categorization-rfs4000)#
nx9500-6C8809(config-device-categorization-rfs4000)#no mark-device 1 sanctioned ap mac
11-22-33-44-55-66

```

The following example shows the device categorization list 'rfs7000' settings after the 'no' command is executed:

```
nx9500-6C8809(config-device-categorization-rfs4000)#show context
device-categorization rfs4000
nx9500-6C8809(config-device-categorization-rfs4000)#
```

### *dhcp-server-policy*

Configures DHCPv4 server policy parameters, such as class, address range, and options. A new policy is created if it does not exist.

#### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### **Syntax**

```
dhcp-server-policy <DHCP-SERVER-POLICY-NAME>
```

#### **Parameters**

```
dhcp-server-policy <DHCP-SERVER-POLICY-NAME>
```

<DHCP-POLICY-NAME> Specify the DHCP server policy name. If the policy does not exist, it is created.

#### **Examples**

```
nx9500-6C8809(config)#dhcp-server-policy test
nx9500-6C8809(config-dhcp-policy-test)#?
DHCP policy Mode commands:
 bootp BOOTP specific configuration
 dhcp-class Configure DHCP class (for address allocation using DHCP
 user-class options)
 dhcp-pool Configure DHCP server address pool
 dhcp-server Activating dhcp server based on criteria
 no Negate a command or set its defaults
 option Define DHCP server option
 ping Specify ping parameters used by DHCP Server

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-dhcp-policy-test)#
```



## Related Commands

|                 |                                        |
|-----------------|----------------------------------------|
| <code>no</code> | Removes an existing DHCP server policy |
|-----------------|----------------------------------------|



### Note

For more information on DHCP policy, see [DHCP-SERVER-POLICY](#).

## *dhcpv6-server-policy*

Creates a DHCPv6 server policy and enters its configuration mode

DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes, or other configuration attributes required on an IPv6 network.

DHCPv6 servers pass IPv6 network addresses to IPv6 clients. The DHCPv6 address assignment feature manages non-duplicate addresses in the correct prefix based on the network where the host is connected. Assigned addresses can be from one or multiple pools. Additional options, such as the default domain and DNS name-server address, can be passed back to the client. Address pools can be assigned for use on a specific interface or on multiple interfaces, or the server can automatically find the appropriate pool.

When configured and applied to a device, the DHCPv6 server policy enables the device to function as a stateless DHCPv6 server.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
dhcpv6-server-policy <DHCPv6-SERVER-POLICY-NAME>
```

### Parameters

```
dhcpv6-server-policy <DHCPv6-SERVER-POLICY-NAME>
```

|                             |                                                                                     |
|-----------------------------|-------------------------------------------------------------------------------------|
| <DHCPv6-SERVER-POLICY-NAME> | Specify the DHCPv6 server policy name. If the policy does not exist, it is created. |
|-----------------------------|-------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config)#dhcpv6-server-policy test
nx9500-6C8809(config-dhcpv6-server-policy-test)#?
DHCPv6 server policy Mode commands:
 dhcpv6-pool Configure DHCPV6 server address pool
 no Negate a command or set its defaults
 option Define DHCPv6 server option
 restrict-vendor-options Restrict vendor specific options to be sent in
 server reply
 server-preference Server preference value sent in the reply, by the
 server to client

 clrscr Clears the display screen
```

```

commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

```

```
nx9500-6C8809(config-dhcpv6-server-policy-test)#
```

### Related Commands

|                 |                                          |
|-----------------|------------------------------------------|
| <code>no</code> | Removes an existing DHCPv6 server policy |
|-----------------|------------------------------------------|



#### Note

For more information on DHCP policy, see [DHCP-SERVER-POLICY](#).

### *dns-whitelist*

Configures a DNS whitelist. A DNS whitelist is a list of allowed DNS destination IP addresses pre-approved to access a controller, service platform, or access point managed captive portal.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
dns-whitelist <DNS-WHITELIST-NAME>
```

#### Parameters

```
dns-whitelist <DNS-WHITELIST-NAME>
```

|                                         |                                                                                 |
|-----------------------------------------|---------------------------------------------------------------------------------|
| <code>&lt;DNS-WHITELIST-NAME&gt;</code> | Specify the DNS whitelist name. If the whitelist does not exist, it is created. |
|-----------------------------------------|---------------------------------------------------------------------------------|

#### Examples

```

nx9500-6C8809(config)#dns-whitelist test
nx9500-6C8809(config-dns-whitelist-test)#?
DNS Whitelist Mode commands:
 no Negate a command or set its defaults
 permit Match a host

 clrscr Clears the display screen
 commit Commit all changes made in this session
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

```

```
nx9500-6C8809(config-dns-whitelist-test)#
```

### Related Commands

|                 |                                   |
|-----------------|-----------------------------------|
| <code>no</code> | Removes an existing DNS Whitelist |
|-----------------|-----------------------------------|

### dns-whitelist-mode-commands

The following table summarizes DNS Whitelist configuration mode commands:

**Table 17: DNS-Whitelist Config Mode Commands**

| Command                                                 | Description                                                                          |
|---------------------------------------------------------|--------------------------------------------------------------------------------------|
| <code>permit</code> on page 375                         | Permits a host, existing on a DNS whitelist, access to the network or captive portal |
| <code>no (dns-whitelist-config-mode)</code> on page 376 | Negates a command or reverts to default                                              |

### permit

A whitelist is a list of host names and IP addresses permitted access to the network or captive portal. This command adds a host or destination IP address to the DNS whitelist.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
permit <IPv4/IPv6/HOSTNAME> {suffix}
```

### Parameters

```
permit <IPv4/IPv6/HOSTNAME> {suffix}
```

|                          |                                                                                                                                                                                                                                                                                                     |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IPv4/IPv6/<br>HOSTNAME> | Adds a device to the DNS whitelist <ul style="list-style-type: none"><li>• &lt;IPv4/IPv6/HOSTNAME&gt; - Provide a hostname or numerical IPv4 or IPv6 address for each destination IP address or host included in the whitelist.</li></ul> <p><b>Note:</b> A maximum of 256 entries can be made.</p> |
| suffix                   | Optional. Matches any hostname including the specified name as suffix                                                                                                                                                                                                                               |

### Examples

```
nx9500-6C8809(config-dns-whitelist-test)#permit example_company.com suffix
nx9500-6C8809(config-dns-whitelist-test)#show context
dns-whitelist test
permit example_company.com suffix
nx9500-6C8809(config-dns-whitelist-test)#
```

### Related Commands

|                 |                               |
|-----------------|-------------------------------|
| <code>no</code> | Removes a DNS whitelist entry |
|-----------------|-------------------------------|

no (dns-whitelist-config-mode)

Removes a specified host or IP address from the DNS whitelist, and prevents it from accessing network resources

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
no permit <IPv4/IPv6/HOSTNAME>
```

#### Parameters

```
no permit <IPv4/IPv6/HOSTNAME>
```

|                      |                                                                                                                                                                                                                                  |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IPv4/IPv6/HOSTNAME> | Removes a device from the DNS whitelist (identifies the device by its IP address or hostname) <ul style="list-style-type: none"><li>• &lt;IPv4/IPv6/HOSTNAME&gt; - Specify the device's IPv4/IPv6 address or hostname.</li></ul> |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config-dns-whitelist-test)#show context
dns-whitelist test
permit example_company.com suffix
nx9500-6C8809(config-dns-whitelist-test)#
nx9500-6C8809(config-dns-whitelist-test)#no permit example_company.com
nx9500-6C8809(config-dns-whitelist-test)#show context
dns-whitelist test
nx9500-6C8809(config-dns-whitelist-test)#
```

*end*

Ends and exits the current mode and moves to the PRIV EXEC mode

The prompt changes to the PRIV EXEC mode.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
end
```

#### Parameters

None

#### Examples

```
rfs4000-229D58(config)#end
rfs4000-229D58#
```

## event-system-policy

Configures a system wide events handling policy

Event system policies enable administrators to create notification mechanisms using one, some, or all of the SNMP, syslog, controller forwarding, or email notification options available to the controller or service platform. Each listed event can have customized notification settings defined and saved as part of an event policy. Thus, policies can be configured and administrated in respect to specific sets of client association, authentication or encryption, and performance events. Once policies are defined, they can be mapped to device profiles strategically as the likelihood of an event applies to particular devices.

To view an existing event system policy configuration details, use the **show > event-system-policy** command.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
event-system-policy <EVENT-SYSTEM-POLICY-NAME>
```

### Parameters

```
event-system-policy <EVENT-SYSTEM-POLICY-NAME>
```

|                                                                                                               |
|---------------------------------------------------------------------------------------------------------------|
| <EVENT-SYSTEM-POLICY-NAME> Specify the event system policy name. If the policy does not exist, it is created. |
|---------------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config)#event-system-policy event-testpolicy
nx9500-6C8809(config-event-system-policy-event-testpolicy)#?
Event System Policy Mode commands:
 event Configure an event
 no Negate a command or set its defaults

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-event-system-policy-event-testpolicy)#
```

### Related Commands

|                                                   |
|---------------------------------------------------|
| <b>no</b> Removes an existing event system policy |
|---------------------------------------------------|

## event-system-policy-mode-commands

The following table summarizes event system policy configuration mode commands:

Table: Event-System-Policy Config Mode Commands

| Command | Description                             |
|---------|-----------------------------------------|
| event   | Configures an event                     |
| no      | Negates a command or reverts to default |

event

Configures an event and sets the action performed when the event happens

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
event <EVENT-TYPE> <EVENT-NAME> (email,forward-to-switch,snmp,syslog) [default|on|off]
```

The even types are:

```
nx9500-6C8809(config-event-system-policy-testpolicy)#event ?
aaa AAA/Radius module
adapt Adaptivity Module
adopt-service Adoption Service
adv-wips Adv-wips module
ap Access Point module
bt Bluetooth
captive-portal Captive Portal
cdp Cisco Discovery Protocol
certmgr Certificate Manager (Not valid for NCAP/MCN)
cfgd Cfgd module
cluster Cluster module
crm Critical Resource Monitoring
database Database Services
device Device module
dhcpcsvr DHCP Configuration Daemon
diag Diag module
dot11 802.11 management module
dot1x 802.1X Authentication
fwu Firmware update module
isdn Isdn module
l2gre Layer 2 GRE Tunnel
l2tpv3 Layer 2 Tunneling Protocol Version 3
licmgr License module
lldp Link Layer Discovery Protocol
mesh Mesh module
mgmt Management Services
nsm Network Services Module
pm Process-monitor module
radconf Radius Configuration Daemon
rasst Roaming-Assist module
radio Radio module
smrt Smart-rf module
smtpnot Smtplot module
system System module
```

```

test Test module
vrrp Virtual Router Redundancy Protocol
webf Webf module
wips Wireless IPS module

```

```
nx9500-6C8809(config-event-system-policy-testpolicy)#
```



**Note**

The parameter values for <EVENT-TYPE> and <EVENT-NAME> are summarized in the table under the Parameters section.

Parameters

```
event <EVENT-TYPE> <EVENT-NAME> (email,forward-to-switch,snmp,syslog) [default|on|off]
```

| <event-type>   | <event-name>                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| aaa            | Enables and configures logging of the following authentication, authorization, and accounting related events: <ul style="list-style-type: none"> <li>radius-discon-msg - RADIUS disconnection message</li> <li>radius-session-expired - RADIUS session expired message</li> <li>radius-session-not-started - RADIUS session not started message</li> <li>radius-vlan-update - RADIUS VLAN update message</li> </ul> |
| adapt          | Enables and configures logging of the following adaptivity module related events: <ul style="list-style-type: none"> <li>adaptivity-change - Event adaptivity change</li> <li>adaptivity-rehome - Event adaptivity rehome</li> </ul>                                                                                                                                                                                |
| adopt-services | Enables and configures the logging of adopted services related events                                                                                                                                                                                                                                                                                                                                               |
| adv-wips       | Enables and configures the logging of advanced WIPS related events                                                                                                                                                                                                                                                                                                                                                  |

| <event-type>   | <event-name>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ap             | Enables and configures logging of the following AP related events: <ul style="list-style-type: none"> <li>• adopted – Event AP adopted</li> <li>• adopted-to-controller – Event AP adopted to wireless controller</li> <li>• ap-adopted – Event access port adopted</li> <li>• ap-autoup-done – Event AP autoup done</li> <li>• ap-autoup-fail – Event AP autoup fail</li> <li>• ap-autoup-needed – Event AP autoup needed</li> <li>• ap-autoup-no-need – Event AP autoup not needed</li> <li>• ap-autoup-reboot – Event AP autoup reboot</li> <li>• ap-autoup-timeout – Event AP autoup timeout</li> <li>• ap-autoup-ver – Event AP autoup version</li> <li>• ap-reset-detected – Event access port reset detected</li> <li>• ap-reset-request – Event access port user requested reset</li> <li>• ap-timeout – Event access port timed out</li> <li>• ap-unadopted – Event access port unadopted</li> <li>• image-parse-failure – Event image parse failure</li> <li>• legacy-auto-update – Event legacy auto update</li> <li>• no-image-file – Event no image file</li> <li>• offline – Event AP detected as offline</li> <li>• online – Event offline AP detected as online</li> <li>• reset – Event reset</li> <li>• sw-conn-lost – Event software connection lost</li> <li>• unadopted – Event unadopted</li> </ul> |
| bt             | Enables and configures logging of the following bluetooth related events: <ul style="list-style-type: none"> <li>• bt-started – Event bluetooth (bt) started</li> <li>• bt-state-change – Event bt state change</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| captive-portal | Enables and configures logging of the following captive portal (hotspot) related events: <ul style="list-style-type: none"> <li>• allow-access – Event client allowed access</li> <li>• auth-failed – Event client authentication failed</li> <li>• auth-success – Event client authentication success</li> <li>• client-disconnect – Event client disconnected</li> <li>• client-removed – Event client removed</li> <li>• data-limit-exceed – Event client data limit exceeded</li> <li>• flex-log-access – Event flexible log access granted to client</li> <li>• inactivity-timeout – Event client time-out due to inactivity</li> <li>• page-cre-failed – Event page creation failure</li> <li>• purge-client – Event client purged</li> <li>• session-timeout – Event session timeout</li> <li>• vlan-switch – Event client switched VLAN</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| cdp            | Enables and configures logging of the following CDP (CISCO Discovery Protocol) related event: <ul style="list-style-type: none"> <li>• duplex-mismatch – Event duplex mismatch detected between CDP neighbors</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |



| <event-type> | <event-name>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| certmgr      | Enables and configures logging of the following certificate manager related events : <ul style="list-style-type: none"> <li>• ca-cert-actions-failure – Event CA certificate actions failure</li> <li>• ca-cert-actions-success – Event CA certificate actions success</li> <li>• ca-key-actions-failure – Event CA key actions failure</li> <li>• ca-key-actions-success – Event CA key actions success</li> <li>• cert-expiry – Event certificate expiry</li> <li>• crl-actions-failure – Event CRL (Certificate Revocation List) actions failure</li> <li>• crl-actions-success – Event CRL actions success</li> <li>• csr-export-failure – Event CSR export failure</li> <li>• csr-export-success – Event CSR export success</li> <li>• delete-trustpoint-action – Event delete trustpoint action</li> <li>• export-trustpoint – Event trustpoint exported</li> <li>• import-trustpoint – Event trustpoint imported</li> <li>• rsa-key-actions-failure – Event RSA key actions failure</li> <li>• rsa-key-actions-success – Event RSA key actions success</li> <li>• svr-cert-actions-success – Event server certificate actions success</li> <li>• svr-cert-actions-failure – Event server certificate actions failure</li> </ul> |
| certmgr-lite | Enables and configures logging of certificate manager (lite version) related event messages                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| cfgd         | Enables and configures logging of the following configuration daemon module related events: <ul style="list-style-type: none"> <li>• acl-attached-altered – Event ACL (Access List ) attached altered</li> <li>• acl-rule-altered – Event ACL rule altered</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| cluster      | Enables and configures logging of the following cluster module related events: <ul style="list-style-type: none"> <li>• cmaster-cfg-update-fail – Event cluster master config update failed</li> <li>• max-exceeded – Event maximum cluster count exceeded</li> <li>• state-change – Event cluster state change (active/inactive)</li> <li>• state-change-active – Event cluster state change to active</li> <li>• state-change-inactive – Event cluster state change to inactive</li> <li>• state-retain-active – Event cluster state retained as active</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| crm          | Enables and configures logging of the following CRM (Critical Resource Monitoring ) related event <ul style="list-style-type: none"> <li>• critical-resource-down – Event critical resource goes down</li> <li>• critical-resource-up – Event critical resource comes up</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| device       | Enables and configures the logging of device module related events                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

| <event-type> | <event-name>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| database     | <p>Enables and configures logging of the following error conditions in the captive-portal/NSight database:</p> <ul style="list-style-type: none"> <li>• database-election-fail – Event primary database node selection failure. Requires manual intervention to select primary database node.</li> <li>• database-exception – Event database may need to be dropped and device restarted</li> <li>• database-low-disk-space – Event database low disk space</li> <li>• Database-new-state – Event database state change</li> <li>• database-op-failure – Event database failure</li> <li>• database-set-name-mismatch – Event replica-set not enabled on host</li> <li>• database-storage-mismatch – Event database mismatch. All database files must be removed.</li> <li>• operation-complete – Event database operation completed successfully</li> <li>• operation-failed – Event database operation failure</li> </ul> |
| dhcpsvr      | <p>Enables and configures logging of the following DHCP server related events:</p> <ul style="list-style-type: none"> <li>• dhcp-start – Event DHCP server started</li> <li>• dhcpsvr-stop – Event DHCP sever stopped</li> <li>• relay-iface-no-ip – Event no IP address on DHCP relay interface</li> <li>• relay-no-iface – Event no interface for DHCP relay</li> <li>• relay-start – Event relay agent started</li> <li>• relay-stop – Event DHCP relay agent stopped</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                         |

| <event-type> | <event-name>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| diag         | <p>Enables and configures logging of the following diagnostics module related events:</p> <ul style="list-style-type: none"> <li>• autogen-tech-sprt – Event autogen technical support</li> <li>• buf-usage – Event buffer usage</li> <li>• cpu-load – Event CPU load</li> <li>• cpu-usage-too-high – Event CPU usage high</li> <li>• cpu-usage-too-high-recovery – Event recovery from high CPU usage</li> <li>• disk-usage – Event disk usage</li> <li>• elapsed-time – Event elapsed time</li> <li>• fan-underspeed – Event fan underspeed</li> <li>• fd-count – Event forward count</li> <li>• free-flash-disk – Event free flash disk</li> <li>• free-flash-inodes – Event free flash inodes</li> <li>• free-nvram-disk – Event free nvram disk</li> <li>• free-nvram-inodes – Event free nvram inodes</li> <li>• free-ram – Event free ram</li> <li>• free-ram-disk – Event free ram disk</li> <li>• free-ram-inodes – Event free ram inodes</li> <li>• head-cache-usage – Event head cache usage</li> <li>• high-temp – Event high temp</li> <li>• ip-dest-usage – Event ip destination usage</li> <li>• led-identify – Event led identify</li> <li>• low-temp – Event low temp</li> <li>• mem-usage-too-high – Event memory usage high</li> <li>• mem-usage-too-high-recovery – Event recovery from high memory usage</li> <li>• new-led-state – Event new led state</li> <li>• over-temp – Event over temp</li> <li>• over-voltage – Event over voltage</li> <li>• poe-init-fail – Event PoE init fail</li> <li>• poe-power-level – Event PoE power level</li> <li>• poe-read-fail – Event PoE read fail</li> <li>• poe-state-change – Event PoE state change</li> <li>• poe-state-change – Event PoE state change</li> <li>• pwrsply-fail – Event failure of power supply</li> <li>• raid-degraded – Event RAID (Redundant Array of Independent Disks) degraded</li> <li>• raid-error – Event RAID error</li> <li>• ram-usage – Event ram usage</li> <li>• under-voltage – Event under voltage</li> <li>• wd-reset-sys – Event wd reset system</li> <li>• wd-state-change – Event wd state change</li> </ul> |

| <event-type> | <event-name>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dot11        | <p>Enables and configures logging of the following 802.11 management module related events:</p> <ul style="list-style-type: none"> <li>• client-assoc-ignored – Wireless client association ignored event</li> <li>• client-associated – Wireless client associated event</li> <li>• client-denied-assoc – Event client denied association</li> <li>• client-disassociated – Wireless client disassociated</li> <li>• country-code – Event country code applied</li> <li>• country-code-error – Event country code error</li> <li>• eap-cached-keys – Event EAP (Extensible Authentication Protocol) cached keys</li> <li>• eap-client-timeout – Event EAP client timeout</li> <li>• eap-failed – Event EAP failed</li> <li>• eap-opp-cached-keys – Event EAP opp cached keys</li> <li>• eap-preauth-client-timeout – Event EAP pre authentication client timeout</li> <li>• eap-preauth-failed – Event EAP pre authentication failed</li> <li>• eap-preauth-server-timeout – Event EAP pre authentication server timeout</li> <li>• eap-preauth-success – Event EAP pre authentication success</li> <li>• eap-server-timeout – Event EAP server timeout</li> <li>• eap-success – Event EAP success</li> <li>• ft-roam-success – Event client fast BSS transition</li> <li>• gal-rx-request – Event GAL request received event</li> <li>• gal-tx-response – Event response sent to GAL request</li> <li>• gal-validate-failed – Event GAL validation failed</li> <li>• gal-validate-req – Event GAL validation request</li> <li>• gal-validate-success – Event GAL validation success</li> <li>• kerberos-client-success – Event client Kerberos authentication success</li> <li>• kerberos-wlan-failed – Event WLAN Kerberos authentication failed</li> <li>• kerberos-wlan-success – Event WLAN Kerberos authentication success</li> <li>• kerberos-wlan-timeout – Event Kerberos authentication timed out</li> <li>• move-operation-success – Event move operation success</li> <li>• tkip-cntrmeas-end – Event TKIP countermeasures ended</li> <li>• tkip-cntrmeas-start – Event TKIP countermeasures initiated</li> <li>• tkip-mic-fail-report – Event TKIP MIC failure report</li> <li>• tkip-mic-failure – Event TKIP MIC check failed</li> <li>• neighbor-denied-assoc – Event neighbor denied association</li> <li>• unsanctioned-ap-active – Event unsanctioned AP active</li> <li>• unsanctioned-ap-inactive – Event unsanctioned AP inactive</li> <li>• unsanctioned-ap-status-change – Event unsanctioned AP status change</li> <li>• voice-call-completed – Event voice call completed</li> <li>• voice-call-established – Event voice call established</li> <li>• voice-call-failed – Event voice call failed</li> <li>• wlan-time-access-disable – Event WLAN disabled by time-based-access</li> <li>• wlan-time-access-enable – Event WLAN re-enabled by time-based-access</li> <li>• wpa-wpa2-failed – Event WPA-WPA2 failed</li> <li>• wpa-wpa2-key-rotn – Event WPA-WPA2 key rotn</li> <li>• wpa-wpa2-success – Event WPA-WPA2 success</li> </ul> |

| <event-type> | <event-name>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dot1x        | Enables and configures logging of the following 802.1X authentication related events: <ul style="list-style-type: none"> <li>• dot1x-failed – Event EAP authentication failure</li> <li>• dot1x-success – Event dot1x-success</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| fwu          | Enables and configures logging of the following fwu (firmware update) related events: <ul style="list-style-type: none"> <li>• fwuaborted – Event fwu aborted</li> <li>• fwubadconfig – Event fwu aborted due to bad config</li> <li>• fwucorruptedfile – Event fwu aborted due to corrupted file</li> <li>• fwucouldntgetfile – Event fwu aborted because the system could not get file</li> <li>• fwudone – Event fwu done</li> <li>• fwufileundef – Event fwu aborted due to file undefined</li> <li>• fwunoneed – Event fwu no need</li> <li>• fwuprodismatch – Event fwu aborted due to product mismatch</li> <li>• fwuserverundef – Event fwu aborted due to server undefined</li> <li>• fwuserverunreachable – Event fwu aborted due to server unreachable</li> <li>• fwusignismatch – Event fwu aborted due to signature mismatch</li> <li>• fwusyserr – Event fwu aborted due to system error</li> <li>• fwuunsupportedhw – Event fwu aborted due to unsupported hardware</li> <li>• fwuunsupportedmodelnum – Event fwu aborted due to unsupported FIPS model number</li> <li>• fwuvermismatch – Event fwu aborted due to version mismatch</li> </ul> |
| isdn         | Configures file ISDN (Integrated Service Digital Network ) module related event s <ul style="list-style-type: none"> <li>• isdn-alert – Event ISDN alert</li> <li>• isdn-crit – Event ISDN critical</li> <li>• isdn-debug – Event ISDN debug</li> <li>• isdn-emerg – Event ISDN emergency</li> <li>• isdn-err – Event ISDN error</li> <li>• isdn-info – Event ISDN info</li> <li>• isdn-notice – Event ISDN notice</li> <li>• isdn-warning – Event ISDN warning</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| l2gre        | Enables and configures logging of the following L2GRE (Layer 2 GRE) tunnel related events: <ul style="list-style-type: none"> <li>• l2gre-tunnel-down – Event L2GRE tunnel down</li> <li>• l2gre-tunnel-failover – Event L2GRE tunnel failover</li> <li>• l2gre-tunnel-up – Event L2GRE tunnel up</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| l2tpv3       | Enables and configures logging of the following Layer 2 GRE (L2GRE) tunnel related events: <ul style="list-style-type: none"> <li>• l2tpv3-tunnel-down – Event L2TPv3 tunnel down</li> <li>• l2tpv3-tunnel-up – Event L2TPv3 tunnel up</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| licmgr       | Enables and configures logging of the following license manager module related events: <ul style="list-style-type: none"> <li>• lic-installed-count – Event total number of license installed count</li> <li>• lic-installed-default – Event default license installation</li> <li>• lic-installed – Event license installed</li> <li>• lic-invalid – Event license installation failed</li> <li>• lic-removed – Event license removed</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

| <event-type> | <event-name>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| lldp         | Enables and configures logging of the following LLDP (Link Layer Discovery Protocol) related events: <ul style="list-style-type: none"> <li>• lldp-loop-detected – Event layer 2 switching loop</li> <li>• lldp-loop-recovery – Event recovery from layer 2 switching loop</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| mgmt         | Enables and configures logging of the following management services module related events: <ul style="list-style-type: none"> <li>• log-http-init – Event Web server started</li> <li>• log-http-local-start – Event Web server started in local mode</li> <li>• log-http-start – Event Web server started in external mode</li> <li>• log-https-start – Event secure Web server started</li> <li>• log-https-wait – Event waiting for Web server to start</li> <li>• log-key-deleted – Event RSA key associated with SSH is deleted</li> <li>• log-key-restored – Event RSA key associated with SSH is added</li> <li>• log-trustpoint-deleted – Event trustpoint associated with HTTPS is deleted</li> </ul>                                                                                                    |
| mesh         | Enables and configures logging of the following mesh module related events: <ul style="list-style-type: none"> <li>• mesh-link-down – Event mesh link down</li> <li>• mesh-link-up – Event mesh link up</li> <li>• meshpoint-down – Event meshpoint down</li> <li>• meshpoint-loop-prevent-off – Event meshpoint loop prevent off</li> <li>• meshpoint-loop-prevent-on – Event meshpoint loop prevent on</li> <li>• meshpoint-path-change – Event meshpoint-path-change</li> <li>• meshpoint-root-change – Event meshpoint-root-change</li> <li>• meshpoint-up – Event meshpoint up</li> </ul>                                                                                                                                                                                                                    |
| nsm          | Configures NSM (Network Service Module) related event <ul style="list-style-type: none"> <li>• dhcpc-err – Event DHCP certification error</li> <li>• dhcpcdefrt – Event DHCP defrt</li> <li>• dhcpcip – Event DHCP IP</li> <li>• dhcpcipchg – Event DHCP IP change</li> <li>• dhcpcipnoadd – Event DHCP IP overlaps static IP address</li> <li>• dhcpcplsexp – Event DHCP lease expiry</li> <li>• dhcpcpnak – Event DHCP server returned DHCP NAK response</li> <li>• dhcpcnodeftrt – Event interface no default route</li> <li>• if-failback – Event interface failback</li> <li>• if-failover – Event interface failover</li> <li>• ifdown – Event interface down</li> <li>• ifipcfg – Event interface IP config</li> <li>• ifup – Event interface up</li> <li>• nsm-ntp – Event translate host name</li> </ul> |

| <event-type> | <event-name>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| pm           | Configures process monitor module related event s <ul style="list-style-type: none"> <li>• procid – Event proc ID generated</li> <li>• procmaxrstrt – Event proc max restart</li> <li>• procnorep – Event proc no response</li> <li>• procrstrt – Event proc restart</li> <li>• procstart – Event proc start</li> <li>• procstop – Event proc stop</li> <li>• procsysrstrt – Event proc system restart</li> <li>• startupcomplete – Event startup complete</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| radconf      | Enables and configures logging of the following RADIUS configuration daemon related events: <ul style="list-style-type: none"> <li>• could-not-stop-radius – Event could not stop RADIUS server</li> <li>• radiusdstart – Event RADIUS server started</li> <li>• radiusdstop – Event RADIUS server stopped</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| radio        | Enables and configures logging of the following radio module related events: <ul style="list-style-type: none"> <li>• acs-scan-complete – Event ACS scan completed</li> <li>• acs-scan-started – Event ACS scan started</li> <li>• cb-associated – Event client-bridge access point associates with an infrastructure access point</li> <li>• cb-roam – Event client-bridge access point roams from one infrastructure access point to another infrastructure access point</li> <li>• cb-wired-client-added – Event wired client is added to the client-bridge</li> <li>• cb-wired-client-removed – Event wired client is removed from the client-bridge</li> <li>• channel-country-mismatch – Event channel and country of operation mismatch</li> <li>• radar-det-info – Detected radar info</li> <li>• radar-detected – Event radar detected</li> <li>• radar-scan-completed – Event radar scan completed</li> <li>• radar-scan-started – Event radar scan started</li> <li>• radio-antenna-error – Event invalid antenna type on this radio</li> <li>• radio-antenna-setting – Event antenna type setting on this radio</li> <li>• radio-state-change – Event radio state change</li> <li>• resume-home-channel – Event resume home channel</li> </ul> |
| rasst        | Enables and configures the logging of roaming assist module related events                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| smrt         | Enables and configures logging of the following SMART RF module related events: <ul style="list-style-type: none"> <li>• calibration-done – Event calibration done</li> <li>• calibration-started – Event calibration started</li> <li>• channel-change – Event channel change</li> <li>• config-cleared – Configuration cleared event</li> <li>• cov-hole-recovery – Event coverage hole recovery</li> <li>• cov-hole-recovery-done – Event coverage hole recovery done</li> <li>• interference-recovery – Event interference recovery</li> <li>• neighbor-recovery – Event neighbor recovery</li> <li>• power-adjustment – Event power adjustment</li> <li>• root-recovery – Event meshpoint root recovery</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| <event-type> | <event-name>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| smtpnot      | <p>Enables and configures logging of the following SMTP module related events:</p> <ul style="list-style-type: none"> <li>• cfg – Event cfg</li> <li>• cfginc – Event cfg inc</li> <li>• net – Event net</li> <li>• proto – Event proto</li> <li>• smtpauth – Event SMTP authentication</li> <li>• smtperr – Event SMTP error</li> <li>• smtpinfo – Event SMTP information</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| system       | <p>Enables and configures logging of the following system module related events:</p> <ul style="list-style-type: none"> <li>• clock-reset – Event clock reset</li> <li>• cold-start – Event cold start</li> <li>• config-commit – Event configuration commit</li> <li>• config-revision – Event config-revision done</li> <li>• devup-rfd-fail – Event device-upgrade failed on rf-domain manager managed devices</li> <li>• guest-user-exp – Event guest user purging</li> <li>• http-err – Event Web server did not start</li> <li>• login – Event successful login</li> <li>• login-fail – Event login fail. Occurs when user authentication fails.</li> <li>• login-fail-access – Event login fail access. Occurs in case of access violation.</li> <li>• login-fail-bad-role – Event login fail bad role. Occurs when user uses an invalid role to logon.</li> <li>• login-lockout – Event user account locked out message. Occurs when a user account is locked due to exceeding of maximum number failed login attempts threshold. Configure this event notification only if the max-fail and lockout-time parameters have been configured in the management-policy context. For more information, see <a href="#">password-entry</a> on page 1530.</li> <li>• login-unlocked – Event user account un-locked. Occurs when a locked user account is re-activated. Enable this event notification only if the max-fail and lockout-time parameters have been configured in the management-policy context. For more information, see <a href="#">password-entry</a> on page 1530.</li> <li>• logout – Event logout</li> <li>• maat-light – Event action on RIM (Research in Motion) radio(s) from the Maat light module</li> <li>• panic – Event panic</li> <li>• periodic-heart-beat – Event periodic heart beat</li> <li>• procstop – Event proc stop</li> <li>• server-unreachable – Event server-unreachable</li> <li>• system-autoup-disable – Event system autoup disable</li> <li>• system-autoup-enable – Event system autoup enable</li> <li>• t5-config-error – Event t5-config-error</li> <li>• ui-user-auth-fail – Event user authentication fail</li> <li>• ui-user-auth-success – Event user authentication success</li> <li>• warm-start – Event warm start</li> <li>• warm-start-recover – Event recovery from warm start</li> </ul> |



| <event-type> | <event-name>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| test         | Enables and configures logging of the following test module related events: <ul style="list-style-type: none"> <li>• testalert – Event test alert</li> <li>• testargs – Event test arguments</li> <li>• testcrit – Event test critical</li> <li>• testdebug – Event test debug</li> <li>• testemerg – Event test emergency</li> <li>• testerr – Event test error</li> <li>• testinfo – Event test information</li> <li>• testnotice – Event test notice</li> <li>• testwarn – Event test warning</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                        |
| vrrp         | Enables and configures logging of the following VRRP (Virtual Router Redundancy Protocol ) related events: <ul style="list-style-type: none"> <li>• vrrp-monitor-change – Event VRRP monitor link state change</li> <li>• vrrp-state-change – Event VRRP state transition</li> <li>• vrrp-vip-subnet-mismatch – Event VRRP IP not overlapping with an interface addresses</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| webf         | Enables and configures logging of the following Web Filtering (webf) module related events: <ul style="list-style-type: none"> <li>• malform-url-request – Event malformed URL request</li> <li>• no-parent-engine – Event 'no session to URL classification server'</li> <li>• srvr-connect-fail – Event URL classification server unreachable</li> <li>• url-blocked – Event URL blocked</li> <li>• webf-lic-acquired – Event webf license acquired</li> <li>• webf-lic-missing – Event webf license missing</li> <li>• webf-lic-revoked – Event webf license revoked</li> </ul>                                                                                                                                                                                                                                                                                                                                 |
| wips         | Enables and configures logging of the following Wireless IPS module related events: <ul style="list-style-type: none"> <li>• air-termination-active – Event air termination active</li> <li>air-termination-ended – Event air termination ended</li> <li>air-termination-inactive – Event air termination inactive</li> <li>air-termination-initiated – Event air termination initiated</li> <li>rogue-ap-active – Event rogue AP active</li> <li>rogue-ap-inactive – Event rogue AP inactive</li> <li>unsanctioned-ap-active – Event unsanctioned AP active</li> <li>unsanctioned-ap-inactive – Event unsanctioned AP inactive</li> <li>unsanctioned-ap-status-change – Event unsanctioned AP changed state</li> <li>wips-client-blacklisted – Event WIPS client blacklisted</li> <li>• wips-client-rem-blacklist – Event WIPS client rem blacklist</li> <li>• wips-event – Event WIPS event triggered</li> </ul> |
| email        | Sends e-mail notifications to a pre configured e-mail ID                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| <event-type>      | <event-name>                                                                      |
|-------------------|-----------------------------------------------------------------------------------|
| forward-to-switch | Forwards the messages to an external server                                       |
| snmp              | Logs an SNMP event                                                                |
| syslog            | Logs an event to syslog                                                           |
| default           | Performs the default action for the event                                         |
| off               | Switches the event off, when the event happens, and no action is performed        |
| on                | Switches the event on, when the event happens, and the configured action is taken |

### Examples

```
rfs4000-229D58(config-event-system-policy-event-testpolicy)#event aaa radius-discon-msg
email on forward-to-switch default snmp default syslog default
rfs4000-229D58(config-event-system-policy-testpolicy)#show context
event-system-policy test
 event aaa radius-discon-msg email on
rfs4000-229D58(config-event-system-policy-testpolicy)#
nx9500-6C8809(config-event-system-policy-test)#event database database-exception
 syslog default snmp default forward-to-switch default email default
nx9500-6C8809(config-event-system-policy-test)#event database operation-failed syslog
default snmp default forward-to-switch default email default
nx9500-6C8809(config-event-system-policy-test)#show context include-factory | grep
operation-failed
 event database operation-failed syslog default snmp default forward-to-switch default
email default
nx9500-6C8809(config-event-system-policy-test)#
```

### Related Commands

|    |                                     |
|----|-------------------------------------|
| no | Resets or disables event monitoring |
|----|-------------------------------------|

no (event-system-policy-config-mode)

Negates an event monitoring configuration

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
no event <EVENT-TYPE> <EVENT-NAME> [email|forward-to-switch|snmp|syslog] [default|on|off]
```

### Parameters

no <PARAMETERS>

|                 |                                                                                                                                                                                                                           |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| no <PARAMETERS> | Removes event monitoring and message forwarding activity based on the parameters passed<br>The system stops network monitoring for the occurrence of the specified event and no notification is sent if the event occurs. |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
rfs4000-229D58(config-event-system-policy-TestPolicy)#event ap adopted syslog default
rfs4000-229D58(config-event-system-policy-TestPolicy)#no event ap adopted syslog
```

## Related Commands

|                       |                                            |
|-----------------------|--------------------------------------------|
| <a href="#">event</a> | Configures the action taken for each event |
|-----------------------|--------------------------------------------|

## ex3500

Creates an EX3500 time range list and enters its configuration mode

An EX3500 time range list consists of a set of periodic and absolute time range rules. Periodic time ranges recur periodically at specified time periods, such as daily, weekly, weekends, weekdays, and on specific week days, for example on every successive Mondays. Absolute time ranges are not periodic and do not recur. They consist of a range of days during a particular time period (the starting and ending days and time are fixed).

The EX3500 series switch is a Gigabit Ethernet layer 2 switch with either 24 or 48 10/100/1000-BASE-T ports, and four SFP (Small Form-factor Pluggable) transceiver slots for fiber connectivity. The EX3500 series switch can adopt to a WiNG NOC controller and be managed by it. The EX3500 time range values configured here are used in EX3500 MAC ACL firewall rules that filter an EX3500's incoming and outgoing traffic. For more information on creating EX3500 MAC ACL rules, see [ex3500 \(mac-acl-config-commands\)](#) on page 1394 and [access-group](#) on page 1299.

### Supported in the following platforms:

- Service Platforms — NX 95XX, NX 7510

### Syntax

```
ex3500 time-range <TIME-RANGE-NAME>
```

### Parameters

```
ex3500 time-range <TIME-RANGE-NAME>
```

|                                     |                                                                                                                                                                       |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ex3500 time-range <TIME-RANGE-NAME> | Configures EX3500 time range list and enters its configuration mode                                                                                                   |
|                                     | <ul style="list-style-type: none"><li>• &lt;TIME-RANGE-NAME&gt; - Enter a name for this EX3500 time range. If the time range does not exist, it is created.</li></ul> |

### Examples

```
nx9500-6C8809(config)#ex3500 time-range EX3500_TimeRange_02
nx9500-6C8809(config-ex3500-time-range-EX3500_TimeRange_02)#?
EX3500 Time Range Configuration commands:
 absolute Absolute time and date
 no Negate a command or set its defaults
 periodic Periodic time and date

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
```

```
show Show running system information
write Write running configuration to memory or terminal
```

```
nx9500-6C8809(config-ex3500-time-range-EX3500_TimeRange_02)#
```

### Related Commands

|                 |                                     |
|-----------------|-------------------------------------|
| <code>no</code> | Removes this EX3500 time range list |
|-----------------|-------------------------------------|

## ex3500-time-range-config-commands

**Table 18: EX3500 Time Range Config Commands**

| Command                                                     | Description                                                            |
|-------------------------------------------------------------|------------------------------------------------------------------------|
| <code>absolute</code> on page 392                           | Configures an absolute time range rule for this EX3500 time range list |
| <code>periodic</code> on page 393                           | Configures a periodic time range rule for this EX3500 time range list  |
| <code>no (ex3500-time-range-config-mode)</code> on page 395 | Removes this EX3500 time range list settings                           |

### absolute

Configures an absolute time range rule for this EX3500 time range list

Absolute time ranges are not periodic and do not recur. They consist of a range of days during a particular time period.

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 7510

#### Syntax

```
absolute start <0-23> <0-59> <1-31> <MONTH> <2013-2037> {end <0-23> <0-59> <1-31> <MONTH> <2013-2037>}
```

#### Parameters

```
absolute start <0-23> <0-59> <1-31> <MONTH> <2013-2037> {end <0-23> <0-59> <1-31> <MONTH> <2013-2037>}
```

|                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| absolute                                          | Configures an absolute time range rule settings                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| start <0-23> <0-59> <1-31><br><MONTH> <2013-2037> | <p>Configures the start day and time settings</p> <ul style="list-style-type: none"> <li>• &lt;0-23&gt; – Specify the start time from 0 - 23 hours.</li> <li>• &lt;0-59&gt; – Specify the start time from 0 - 59 minutes.</li> </ul> <p>For example, if the values provided are 12 hours and 30 minutes, the start time is 12:30 A.M on the specified day.</p> <ul style="list-style-type: none"> <li>• &lt;1-31&gt; – Specify the day of month from 1 - 31 when the time range starts.</li> <li>• &lt;MONTH&gt; – Specify the month. The options are: April, August, December, February, January, July, June, March, May, November, October, September.</li> <li>• &lt;2013-2037&gt; – Specify the year from 2013 - 2037.</li> </ul> |
| end <0-23> <0-59> <1-31><br><MONTH> <2013-2037>   | <p>Optional. Configures the end day and time settings</p> <ul style="list-style-type: none"> <li>• &lt;0-23&gt; – Specify the end time from 0 - 23 hours.</li> <li>• &lt;0-59&gt; – Specify the end time from 0 - 59 minutes.</li> <li>• &lt;1-31&gt; – Specify the day of month from 1 - 31 when the time range ends.</li> <li>• &lt;MONTH&gt; – Specify the month. The options are: April, August, December, February, January, July, June, March, May, November, October, September.</li> <li>• &lt;2013-2037&gt; – Specify the year from 2013 - 2037.</li> </ul>                                                                                                                                                                  |

#### Examples

```
EX3500(config-ex3500-time-range-EX3500-TimeRange-01)#absolute start 1 0 1
 june 2017 end 1 0 30 june 2018
EX3500(config-ex3500-time-range-EX3500-TimeRange-01)#show context
ex3500 time-range EX3500-TimeRange-01
 absolute start 1 0 1 june 2018 end 1 0 30 june 2018
EX3500(config-ex3500-time-range-EX3500-TimeRange-01)#
```

#### Related Commands

|    |                                                                       |
|----|-----------------------------------------------------------------------|
| no | Removes this absolute time range rule from the EX3500 time range list |
|----|-----------------------------------------------------------------------|

#### periodic

Configures a periodic time range rule for this EX3500 time range list

Periodic time ranges are configured to recur based on periodicity such as daily, weekly, weekends, weekdays, and on specific week days, such as on every successive Sunday.

Supported in the following platforms:

- Service Platforms – NX 95XX, NX 7510

#### Syntax

```
periodic [daily|friday|monday|saturday|sunday|thursday|tuesday|wednesday|weekdays|weekend]
<0-23> <0-59> to [<023> <0-59>|daily|friday|monday|saturday|sunday|thursday|tuesday|
wednesday|
weekdays|weekend] <0-23> <0-59> rule-precedence <1-7>
```

#### Parameters

```
periodic [daily|friday|monday|saturday|sunday|thursday|tuesday|wednesday|weekdays|weekend]
<0-23> <0-59> to [<023> <0-59>|daily|friday|monday|saturday|sunday|thursday|tuesday|
wednesday|
weekdays|weekend] <0-23> <0-59> rule-precedence <1-7>
```

|                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>periodic [daily friday monday saturday sunday thursday tuesday wednesday weekdays weekend]</p>                    | <p>Configures this periodic time range's start day. The options are:</p> <ul style="list-style-type: none"> <li>• daily</li> <li>• Friday</li> <li>• Monday</li> <li>• Saturday</li> <li>• Sunday</li> <li>• Thursday</li> <li>• Tuesday</li> <li>• Wednesday</li> <li>• weekdays</li> <li>• weekend</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <p>&lt;0-23&gt; &lt;0-59&gt;</p>                                                                                     | <p>After specifying the start day, specify the start time in hours (24 hours format) and minutes</p> <ul style="list-style-type: none"> <li>• &lt;0-23&gt; – Specify the start time from 0 - 23 hours. <ul style="list-style-type: none"> <li>• &lt;0-59&gt; – Specify the start time from 0 - 59 minutes.</li> </ul> </li> </ul> <p>For example, if the values provided are 12 hours and 30 minutes, the start time is 12:30 A.M on the specified day.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <p>to [&lt;023&gt; &lt;0-59&gt; daily friday monday saturday sunday thursday tuesday wednesday weekdays weekend]</p> | <p>Configures this periodic time range's end day. This is the day when the time range ends. The options available changes depending on the start day configured. The options are:</p> <ul style="list-style-type: none"> <li>• &lt;0-23&gt; &lt;0-59&gt; – Select this option to end the time range on the same day as it starts. Specify the end hour from 0 - 23 hours and the minutes from 0 - 59 minutes.</li> <li>• daily – Select this option if the time range starts and ends every day at a specified time</li> <li>• friday – Select this option if the time range ends on Fridays</li> <li>• monday – Select this option if the time range ends on Mondays</li> <li>• saturday – Select this option if the time range ends on Saturdays</li> <li>• sunday – Select this option if the time range ends on Sundays</li> <li>• thursday – Select this option if the time range ends on Thursdays</li> <li>• tuesday – Select this option if the time range ends on Tuesdays</li> <li>• wednesday – Select this option if the time range ends on Wednesdays</li> <li>• weekdays – Select this option if the time range ends on Weekdays</li> <li>• weekend – Select this option if the time range ends on Weekends</li> </ul> <p>If the time range does not end on the same day, select the end day, and then specify the end time, or else just specify the end time.</p> |
| <p>&lt;0-23&gt; &lt;0-59&gt;</p>                                                                                     | <p>After specifying the end day, specify the end time in hours (in 24 hours format) and minutes</p> <ul style="list-style-type: none"> <li>• &lt;0-23&gt; – Specify the end time from 0 - 23 hours. <ul style="list-style-type: none"> <li>• &lt;0-59&gt; – Specify the end minute from 0 - 59 minutes.</li> </ul> </li> </ul> <p>In case of time ranges starting and ending on the same day, ensure that the end time (hours and minutes) is not lower than the specified start time.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <p>rule-precedence &lt;1-7&gt;</p>                                                                                   | <p>Configures a precedence value for this periodic time range rule. Rules with lower precedence have higher priority and are applied first.</p> <ul style="list-style-type: none"> <li>• &lt;1-7&gt; – Specify a precedence value from 1 - 7.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

## Examples

```
nx9500-6C8809(config-ex3500-time-range-EX3500-TimeRange-01)#periodic daily 1 10
to daily 23 10 rule-precedence 1
nx9500-6C8809(config-ex3500-time-range-EX3500-TimeRange-01)#show context
ex3500 time-range EX3500-TimeRange-01
 periodic daily 1 10 to daily 23 10 rule-precedence 1
 absolute start 1 0 1 june 2017 end 1 0 30 june 2018
nx9500-6C8809(config-ex3500-time-range-EX3500-TimeRange-01)#
```

## Related Commands

|                 |                                                                       |
|-----------------|-----------------------------------------------------------------------|
| <code>no</code> | Removes this periodic time range rule from the EX3500 time range list |
|-----------------|-----------------------------------------------------------------------|

## no (ex3500-time-range-config-mode)

Removes this EX3500 time range list settings

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 7510

## Syntax

```
no [absolute|periodic]
no absolute
no periodic [daily|friday|monday|saturday|sunday|thursday|tuesday|wednesday|weekdays|
weekend]
<0-23> <0-59> to [<0-23> <0-59>|daily|friday|monday|saturday|sunday|thursday|tuesday|
wednesday|
weekdays|weekend]
```

## Parameters

```
no <PARAMETERS>
```

|                                    |                                                                             |
|------------------------------------|-----------------------------------------------------------------------------|
| <code>no &lt;PARAMETERS&gt;</code> | Removes this EX3500 time range list settings based on the parameters passed |
|------------------------------------|-----------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-ex3500-time-range-EX3500-TimeRange-01)#show context
ex3500 time-range EX3500-TimeRange-01
 periodic daily 1 10 to daily 23 10 rule-precedence 1
 absolute start 1 0 1 june 2017 end 1 0 30 june 2018
nx9500-6C8809(config-ex3500-time-range-EX3500-TimeRange-01)#
nx9500-6C8809(config-ex3500-time-range-EX3500-TimeRange-01)#no periodic daily 1
10 to daily 23 10 rule-precedence 1
nx9500-6C8809(config-ex3500-time-range-EX3500-TimeRange-01)#show context
ex3500 time-range EX3500-TimeRange-01
 absolute start 1 0 1 june 2017 end 1 0 30 june 2018
nx9500-6C8809(config-ex3500-time-range-EX3500-TimeRange-01)#
```

## ex3500-management-policy

Creates an EX3500 management policy and enters its configuration mode. Once configured and applied on a EX3500 switch, the management policy controls access to the switch from management stations using SNMP.

The EX3500 management policy is either applied:

- Individually on an adopted EX3500 series switch (in the device configuration mode), or
- To an EX3524 and EX35XX profile, which is then applied to an adopted EX3500 series switch.

EX3500 devices (EX3524 and EX35XX) are layer 2 Gigabit Ethernet switches with either 24 or 48 10/100/1000-BASE-T ports, and four SFP transceiver slots for fiber connectivity. Each 10/100/1000

Mbps port supports both the IEEE 802.3af and IEEE 802.3at-2009 PoE standards. An EX3500 switch has an SNMP-based management agent that provides both in-band and out-of-band management access. The EX3500 switch utilizes an embedded HTTP Web agent and CLI, which in spite of being different from that of the WiNG operating system provides WiNG controllers PoE and port management resources.

Going forward NX 9500 and NX 7500 WiNG managed series service platforms and WiNG VMs can discover, adopt, and partially manage EX3500 series Ethernet switches without modifying the proprietary operating system running the EX3500 switches. The WiNG service platforms utilize standardized WiNG interfaces to push configuration files to the EX3500 switches, and maintain a translation layer, understood by the EX3500 switch, for statistics retrieval.

WiNG can partially manage an EX3500 without using DHCP option 193, provided the EX3500 is directly configured to specify the IPv4 addresses of potential WiNG adopters. To identify the potential WiNG adopter, in the EX3500's device configuration mode specify the adopter's IPv4 address using the **controller > host > <IP-ADDRESS>** command. WiNG service platforms leave the proprietary operating system running the EX3500 switches unmodified, and partially manage them utilizing standardized WiNG interfaces. WiNG service platforms use a translation layer to communicate with the EX3500.

#### Supported in the following platforms:

- Service Platforms — NX 95XX, NX 7510

#### Syntax

```
ex3500-management-policy <POLICY-NAME>
```

#### Parameters

```
ex3500-management-policy <POLICY-NAME>
```

|               |                                                                                         |
|---------------|-----------------------------------------------------------------------------------------|
| <POLICY-NAME> | Specify the EX3500 management policy name. If the policy does not exist, it is created. |
|---------------|-----------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config)#ex3500-management-policy test
nx9500-6C8809(config-ex3500-management-policy-test)#?
EX3500_Management Mode commands:
 enable Modifies enable password parameters
 http Hyper Text Terminal Protocol (HTTP)
 memory Memory utilization
 no Negate a command or set its defaults
 process-cpu Process-cpu utilization
 snmp-server Enable SNMP server configuration
 ssh Secure Shell server connections
 username Login TACACS server port

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal
```



```
nx9500-6c8809(config-ex3500-management-policy-test)#
```

## Related Commands

|                 |                                       |
|-----------------|---------------------------------------|
| <code>no</code> | Removes this EX3500 management policy |
|-----------------|---------------------------------------|

## ex3500-management-policy-config-commands

**Table 19: EX3500 Management Policy Config Commands**

| Command                  | Description                                                                                                                                                               |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>enable</code>      | Configures an executive password for this EX3500 management policy                                                                                                        |
| <code>http</code>        | Configures the HTTP server settings used to authenticate HTTP connection to a EX3500 switch                                                                               |
| <code>memory</code>      | Configures the EX3500's memory utilization rising (upper) and falling (lower) threshold values                                                                            |
| <code>process-cpu</code> | Configures the EX3500's CPU (processor) utilization rising (upper) and falling (lower) threshold values                                                                   |
| <code>snmp-server</code> | Configures SNMP server settings. Once configured and applied on a EX3500 switch, the management policy controls access to the switch from management stations using SNMP. |
| <code>ssh</code>         | Configures the SSH server settings used to authenticate SSH connection to a EX3500 switch                                                                                 |
| <code>username</code>    | Configures a EX3500 switch user settings                                                                                                                                  |
| <code>no</code>          | Removes or reverts this EX3500 management policy settings                                                                                                                 |

### enable

Configures an executive password for this EX3500 management policy

Each EX3500 management policy can have a unique executive password with its own privilege level assigned. Utilize these passwords as specific EX3500 management sessions require priority over others.

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 7510

#### Syntax

```
enable password [0|7|level]
enable password [0|7] <PASSWORD>
enable password level <0-15> [0 <PASSWORD>|7 <PASSWORD>]
```

#### Parameters

```
enable password [0|7] <PASSWORD>
```

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| enable password [0 7]<br><PASSWORD> | <p>Creates a new executive password for this EX3500 management policy. The password could be in clear text or encrypted</p> <ul style="list-style-type: none"> <li>• 0 - Configures a clear text password using ASCII characters (should be 1 - 32 characters long)</li> <li>• 7 - Configures an encrypted password using HEX characters (should be 32 characters long)</li> <li>• &lt;PASSWORD&gt; - Specify the password.</li> </ul> |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

enable password level <0-15> [0 <PASSWORD>|7 <PASSWORD>]

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| enable password level <0-15> | <p>Creates a new executive password for this EX3500 management policy and sets its privilege level</p> <ul style="list-style-type: none"> <li>• &lt;0-15&gt; - Specify the privilege level for this executive password from 0 - 15. Lower values have higher priority, to slot and prioritize executive passwords and EX3500 management sessions.</li> </ul>                                                           |
| [0 7] <PASSWORD>             | <p>After setting the privilege level, configure the password, which could be in clear text or encrypted</p> <ul style="list-style-type: none"> <li>• 0 - Configures a clear text password using ASCII characters (should be 1 - 32 characters long)</li> <li>• 7 - Configures an encrypted password using HEX characters (should be 32 characters long)</li> <li>• &lt;PASSWORD&gt; - Specify the password.</li> </ul> |

### Examples

```

nx9500-6C8809(config-ex3500-management-policy-test)#enable password level 3 7
12345678901020304050607080929291
nx9500-6C8809(config-ex3500-management-policy-test)#show context
ex3500-management-policy test
 enable password level 3 7 12345678901020304050607080929291
 snmp-server notify-filter 1 remote 127.0.0.1
nx9500-6C8809(config-ex3500-management-policy-test)#

```

### Related Commands

|    |                                                                 |
|----|-----------------------------------------------------------------|
| no | Removes a executive password from this EX3500 management policy |
|----|-----------------------------------------------------------------|

### http

Configures the EX3500's memory utilization rising (upper) and falling (lower) threshold values. Once configured, the system sends a notification when the memory utilization exceeds the specified rising limit or falls below the specified falling limit.

By customizing an EX3500's memory and CPU utilization's upper and lower thresholds, you can avoid over utilization of the EX3500's processor capacity when sharing network resources with an NX series service platform or a WiNG VM.

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 7510

### Syntax

```
memory [falling-threshold|rising-threshold] <1-100>
```

### Parameters

|                              |                                                                                                                                                                                                                        |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| memory                       | Configures the EX3500's memory utilization rising and falling threshold values. The system generates a notification when either of these limits is exceeded.                                                           |
| falling-threshold<br><1-100> | Configures the falling threshold for the EX3500 memory utilization <ul style="list-style-type: none"> <li>• &lt;1-100&gt; - Specify the falling threshold as a percentage from 1 - 100. The default is 70%.</li> </ul> |
| rising-threshold<br><1-100>  | Configures the rising threshold for the EX3500's memory utilization <ul style="list-style-type: none"> <li>• &lt;1-100&gt; - Specify the rising threshold as a percentage from 1 - 100. The default is 90%.</li> </ul> |

#### Examples

```

nx9500-6C8809(config-ex3500-management-policy-test)#http secure-server
nx9500-6C8809(config-ex3500-management-policy-test)#show context
ex3500-management-policy test
 http secure-server
 enable password level 3 7 12345678901020304050607080929291
 snmp-server notify-filter 1 remote 127.0.0.1
nx9500-6C8809(config-ex3500-management-policy-test)#

```

#### Related Commands

|    |                                                                             |
|----|-----------------------------------------------------------------------------|
| no | Reverts to default HTTP server settings (HTTP server enabled, HTTP port 80) |
|----|-----------------------------------------------------------------------------|

#### memory

Configures the EX3500's memory utilization rising (upper) and falling (lower) threshold values. Once configured, the system sends a notification when the memory utilization exceeds the specified rising limit or falls below the specified falling limit.

By customizing an EX3500's memory and CPU utilization's upper and lower thresholds, you can avoid over utilization of the EX3500's processor capacity when sharing network resources with an NX series service platform or a WiNG VM.

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 7510

#### Syntax

```
memory [falling-threshold|rising-threshold] <1-100>
```

#### Parameters

```
memory [falling-threshold|rising-threshold] <1-100>
```

|                           |                                                                                                                                                                                                                        |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| memory                    | Configures the EX3500's memory utilization rising and falling threshold values. The system generates a notification when either of these limits is exceeded.                                                           |
| falling-threshold <1-100> | Configures the falling threshold for the EX3500 memory utilization <ul style="list-style-type: none"> <li>• &lt;1-100&gt; - Specify the falling threshold as a percentage from 1 - 100. The default is 70%.</li> </ul> |
| rising-threshold <1-100>  | Configures the rising threshold for the EX3500's memory utilization <ul style="list-style-type: none"> <li>• &lt;1-100&gt; - Specify the rising threshold as a percentage from 1 - 100. The default is 90%.</li> </ul> |

#### Examples

```

nx9500-6C8809(config-ex3500-management-policy-test)#memory falling-threshold 50
nx9500-6C8809(config-ex3500-management-policy-test)#memory rising-threshold 95
nx9500-6C8809(config-ex3500-management-policy-test)#show context
ex3500-management-policy test

```

```

http secure-server
enable password level 3 7 12345678901020304050607080929291
snmp-server notify-filter 1 remote 127.0.0.1
memory falling-threshold 50
memory rising-threshold 95
nx9500-6C8809(config-ex3500-management-policy-test)#

```

#### Related Commands

|           |                                                                                                        |
|-----------|--------------------------------------------------------------------------------------------------------|
| <b>no</b> | Reverts the memory utilization's falling-threshold and/or rising threshold to 70% and 90% respectively |
|-----------|--------------------------------------------------------------------------------------------------------|

#### process-cpu

Configures the EX3500's CPU (processor) utilization rising (upper) and falling (lower) threshold values. Once configured, the system sends a notification when the CPU utilization exceeds the specified rising limit or falls below the specified falling limit.

By customizing an EX3500's memory and CPU utilization's upper and lower thresholds, you can avoid over utilization of the EX3500's processor capacity when sharing network resources with an NX series service platform or a WiNG VM.

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 7510

#### Syntax

```
process-cpu [falling-threshold|rising-threshold] <1-100>
```

#### Parameters

```
process-cpu [falling-threshold|rising-threshold] <1-100>
```

|                           |                                                                                                                                                                                                                       |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| process-cpu               | Configures the EX3500's CPU utilization rising and falling threshold values. The system generates a notification when either of these limits is exceeded.                                                             |
| falling-threshold <1-100> | Configures the falling threshold for the EX3500's CPU utilization <ul style="list-style-type: none"> <li>• &lt;1-100&gt; - Specify the falling threshold as a percentage from 1 - 100. The default is 70%.</li> </ul> |
| rising-threshold <1-100>  | Configures the rising threshold for the EX3500's CPU utilization <ul style="list-style-type: none"> <li>• &lt;1-100&gt; - Specify the rising threshold as a percentage from 1 - 100. The default is 90%.</li> </ul>   |

#### Example (User Exec Mode)

```

nx9500-6C8809(config-ex3500-management-policy-test)#process-cpu falling-threshold 60
nx9500-6C8809(config-ex3500-management-policy-test)#process-cpu rising-threshold 80
nx9500-6C8809(config-ex3500-management-policy-test)#show context
ex3500-management-policy test
 http secure-server
 enable password level 3 7 12345678901020304050607080929291
 snmp-server notify-filter 1 remote 127.0.0.1
 memory falling-threshold 50
 memory rising-threshold 95
 process-cpu falling-threshold 60
 process-cpu rising-threshold 80
nx9500-6C8809(config-ex3500-management-policy-test)#

```

#### Related Commands

no

Reverts the CPU utilization's falling-threshold and/or rising threshold to 70% and 90% respectively

## snmp-server

Configures SNMP (Simple Network Management Protocol) server settings. Once configured and applied on a EX3500 switch, the management policy controls access to the switch from management stations using SNMP.

SNMP is an application layer protocol that facilitates the exchange of management information between the management stations and a managed EX3500 switch. SNMP-enabled devices listen on port 162 (by default) for SNMP packets from the management server. SNMP uses read-only and read-write community strings as an authentication mechanism to monitor and configure supported devices. The read-only community string is used to gather statistics and configuration parameters from a supported wireless device. The read-write community string is used by a management server to set device parameters. SNMP is generally used to monitor a system's performance and other parameters.

Supported in the following platforms:

- Service Platforms – NX 95XX, NX 7510

### Syntax

```
snmp-server {community|contact|enable|engine-id|group|host|location|notify-filter|
user|view}
snmp-server {community <STRING> {ro|rw}}
snmp-server {contact <NAME>}
snmp-server {enable traps {authentication|link-up-down}}
snmp-server {engine-id [local <WORD>|remote <IP> <WORD>]}
snmp-server {group <GROUP-NAME> [v1|v2c|v3 [auth|noauth|priv]] {notify <WORD>|read <WORD>|
write <WORD>}}
snmp-server {host <IP> [<STRING>|inform]}
snmp-server {host <IP> <STRING> version [v1|v2c|v3 [auth|noauth|priv]]
{udp-port <1-65535>}}
snmp-server {host <IP> inform [retry <0-255>|timeout <0-2147483647>]
<STRING> version [v2c|v3 [auth|noauth|priv]] {udp-port <1-65535>}}
snmp-server {location <WORD>}
snmp-server {notify-filter <WORD> remote <IP>}
snmp-server {user <USER-NAME> <GROUP-NAME> [remote-host|v1|v2c|v3]}
snmp-server {user <USER-NAME> <GROUP-NAME> remote-host <IP> v3 [auth|encrypted auth]
[md5|sha] <WORD> {priv [3des|aes128|aes192|aes256|des56] <WORD>}}
snmp-server {user <USER-NAME> <GROUP-NAME> [v1|v2c|v3]}
snmp-server {view <VIEW-NAME> <OID-TREE-STRING> [excluded|included]}
```

### Parameters

```
snmp-server {community <STRING> {ro|rw}}
```

|                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>snmp-server {community &lt;STRING&gt; {ro rw}}</pre> | <p>Configures SNMP-server related settings</p> <ul style="list-style-type: none"> <li>community – Optional. Configures an SNMP community access string used to authorize management access by clients using SNMP v1, v2c, or v3 <ul style="list-style-type: none"> <li>&lt;STRING&gt; – Specify the SNMP community access string (should not exceed 32 characters).</li> </ul> </li> </ul> <p>After specifying the string, optionally specify the access type associated with it.</p> <ul style="list-style-type: none"> <li>ro – Optional. Provides read-only access with this SNMP community string. Allows authorized clients to only retrieve MIB (Management Information Base) objects. This is the default setting.</li> <li>rw – Optional. Provides read-write access with this SNMP community string. Allows authorized clients to retrieve as well as modify MIB objects.</li> </ul> <p>You can configure a maximum of five (5) community strings per EX3500 management policy.</p> |
|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
snmp-server {contact <NAME>}
```

|                                               |                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>snmp-server {contact &lt;NAME&gt;}</pre> | <p>Configures SNMP-server related settings</p> <ul style="list-style-type: none"> <li>contact – Optional. Configures the system’s contact information <ul style="list-style-type: none"> <li>&lt;NAME&gt; – Specify the contact person’s name (should not exceed 255 characters).</li> </ul> </li> </ul> |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
snmp-server {enable traps {authentication/link-up-down}}
```

|                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>snmp-server {enable traps {authentication link-up-down}}</pre> | <p>Configures SNMP-server related settings</p> <ul style="list-style-type: none"> <li>enable traps – Optional. Enables the EX3500 switch to send following SNMP traps or notifications: <ul style="list-style-type: none"> <li>authentication – Optional. Enables SNMP authentication trap. This option is disabled by default.</li> <li>link-up-down – Optional. Enables SNMP link up and link down traps. This option is disabled by default.</li> </ul> </li> </ul> <p>If the command is executed without either of the above mentioned trap options, the system enables both authentication and link-up-down traps.<br/>If enabling SNMP traps, use the <b>snmp-server &gt; host</b> command to specify the host(s) receiving the SNMP notifications.</p> |
|---------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
snmp-server {engine-id [local <WORD>|remote <IP> <WORD>]}
```

|                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>snmp-server {engine-id [local &lt;WORD&gt; remote &lt;IP&gt; &lt;WORD&gt;]}</pre> | <p>Configures SNMP-server related settings</p> <ul style="list-style-type: none"> <li>engine-id – Optional. Configures an identification string for the SNMPv3 engine. The SNMP engine is an independent SNMP agent residing either on the logged switch or on a remote device. It prevents message replay, delay, and redirection. In SNMPv3, the engine ID in combination with user passwords generates the security keys that is used for SNMPv3 packet authentication and encryption. <ul style="list-style-type: none"> <li>local – Configures the SNMP engine on the logged switch <ul style="list-style-type: none"> <li>&lt;WORD&gt; – Specify the hexadecimal engine ID string identifying the SNMP engine (should be 9 - 64 characters in length).</li> </ul> </li> <li>remote &lt;IP&gt; &lt;WORD&gt; – Configures a remote device as the SNMP engine <ul style="list-style-type: none"> <li>&lt;IP&gt; – Specify the remote device's IP address.</li> <li>&lt;WORD&gt; – Specify the hexadecimal engine ID string identifying the SNMP engine (should be 9 - 64 characters in length).</li> </ul> </li> </ul> </li> </ul> <p>Configure the remote engine ID when using SNMPv3 informs. The remote ID configured here is used to generate the security digest for authentication and encryption of packets exchanged between the switch and the and the remote host user. SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it.</p> |
|----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
snmp-server {group <GROUP-NAME> [v1/v2c/v3 [auth/noauth/priv]] {notify <WORD>/
read <WORD>/write <WORD>}}
```

|                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>snmp-server group &lt;GROUP- NAME&gt;</pre> | <p>Configures SNMP-server related settings</p> <ul style="list-style-type: none"> <li>group – Optional. Configures an SNMP user group, mapping SNMP users to SNMP views <ul style="list-style-type: none"> <li>&lt;GROUP-NAME&gt; – Specify the SNMP group name (should not exceed 32 characters).</li> </ul> </li> </ul>                                                                                                                                                                                                                                                              |
| <pre>[v1/v2c/v3 [auth/noauth/priv]]</pre>        | <p>Configures the SNMP version used for authentication by this user group</p> <ul style="list-style-type: none"> <li>v1 – Configures the SNMP version as v1.</li> <li>v2c – Configures SNMP version as v2c</li> <li>v3 – Configures the SNMP version as v3. If using SNMP v3, specify the authentication and encryption levels. <ul style="list-style-type: none"> <li>auth – Uses SNMP v3 with authentication and no privacy</li> <li>noauth – Uses SNMP v3 with no authentication and no privacy</li> <li>priv – Uses SNMP v3 with authentication and privacy</li> </ul> </li> </ul> |
| <pre>notify &lt;WORD&gt;</pre>                   | <p>Optional. Configures the notification view string</p> <ul style="list-style-type: none"> <li>&lt;WORD&gt; – Specify the string (should not exceed 32 characters).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                        |
| <pre>read &lt;WORD&gt;</pre>                     | <p>Optional. Configures the read view string</p> <ul style="list-style-type: none"> <li>&lt;WORD&gt; – Specify the string (should not exceed 32 characters).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                |
| <pre>write &lt;WORD&gt;</pre>                    | <p>Optional. Configures the write view string</p> <ul style="list-style-type: none"> <li>&lt;WORD&gt; – Specify the string (should not exceed 32 characters).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                               |

```
snmp-server {host <IP> <STRING> version [v1/v2c/v3 [auth/noauth/priv]] {udp-port
<1-65535>}}
```

|                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>snmp-server host &lt;IP&gt;</p> <p>&lt;STRING&gt;</p> | <p>Configures SNMP-server related settings</p> <ul style="list-style-type: none"> <li>• host – Optional. Configures the host(s) receiving the SNMP notifications. At least one SNMP server host should be configured in order to configure the switch to send notifications <ul style="list-style-type: none"> <li>• &lt;IP&gt; – Specify the SNMP host's IP address.</li> </ul> </li> </ul> <p>You can configure a maximum of five (5) SNMP trap recipients per EX3500 management policy.<br/>Ensure that SNMP trap notification is enabled.</p> <p>Configures the SNMP community string. You can configure the SNMP community string here, or else use the string configured using the <b>snmp-server &gt; community &lt;STRING&gt; &gt; {ro rw}</b> command. It is recommended that you configure the SNMP community string prior to configuring the SNMP host.</p> <ul style="list-style-type: none"> <li>• &lt;STRING&gt; – Specify the community string. The string configured here is sent in the SNMP traps to the SNMPv1 or SNMPv2c hosts.</li> </ul> |
| <p>version [v1 v2c  v3 [auth  noauth  priv]]</p>         | <p>Configures the SNMP version used</p> <ul style="list-style-type: none"> <li>• v1 – Configures the SNMP version as 1. This is the default setting.</li> <li>• v2c – Configures SNMP version as 2c</li> <li>• v3 – Configures the SNMP version as 3. If using SNMPv3, specify the authentication and encryption levels. <ul style="list-style-type: none"> <li>• auth – Uses SNMP v3 with authentication and no privacy</li> <li>• noauth – Uses SNMP v3 with no authentication and no privacy</li> <li>• priv – Uses SNMP v3 with authentication and privacy</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <p>udp-port &lt;1-65535&gt;</p>                          | <p>Optional. After specifying the SNMP version, optionally specify the host UDP port</p> <ul style="list-style-type: none"> <li>• &lt;1-65535&gt; – Specify the UDP port. The default is 162.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

```
snmp-server {host <IP> inform [retry <0-255>/timeout <0-2147483647>] <STRING>
version [v2c/v3 [auth/noauth/priv]] {udp-port <1-65535>}}
```



|                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| snmp-server host <IP>                         | <p>Configures SNMP-server related settings</p> <ul style="list-style-type: none"> <li>host - Optional. Configures the host(s) receiving the SNMP notifications <ul style="list-style-type: none"> <li>&lt;IP&gt; - Specify the SNMP host's IP address.</li> </ul> </li> </ul> <p>You can configure a maximum of five (5) SNMP trap recipients per EX3500 management policy.<br/>Ensure that SNMP trap notification is enabled.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| inform [retry <0-255>] timeout <0-2147483647> | <p>Enables sending of SNMP notifications as inform messages, and configures inform message settings.</p> <ul style="list-style-type: none"> <li>retry &lt;0-255&gt; - Configures the maximum number attempts made to re-send an inform message in case the specified SNMP host does not acknowledge receipt. &lt;0-255&gt; - Specify a value from 0 - 255. The default is 3.</li> <li>timeout &lt;0-2147483647&gt; - Configures the interval, in seconds, to wait for an acknowledgment from the SNMP host before re-sending an inform message <ul style="list-style-type: none"> <li>&lt;0-2147483647&gt; - Specify a value from 0 - 2147483647 seconds. The default is 1500 seconds.</li> </ul> </li> </ul> <p>Inform messages are more reliable than trap messages since they include a request for acknowledgement of receipt. Using inform messages to communicate critical information would be good practice. However, since inform messages are retained in the memory until a response is received, they consume more memory and may also result in traffic congestion. Take into considerations these facts when configuring the notification format.</p> |
| <STRING>                                      | <p>Configures the SNMP community string. You can configure the SNMP community string here, or else use the string configured using the <b>snmp-server &gt; community &lt;STRING&gt; &gt; {ro rw}</b> command. It is recommended that you configure the SNMP community string prior to configuring the SNMP host.</p> <ul style="list-style-type: none"> <li>&lt;STRING&gt; - Specify the community string. The string configured here is sent in the SNMP inform messages to the SNMPv2c or SNMPv3 hosts.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| version [v2c  v3 [auth noauth priv]]          | <p>Configures the SNMP version used</p> <ul style="list-style-type: none"> <li>v2c - Configures the SNMP version as v2c</li> <li>v3 - Configures the SNMP version as v3. If using SNMP v3, specify the authentication and encryption levels. <ul style="list-style-type: none"> <li>auth - Uses SNMP v3 with authentication and no privacy</li> <li>noauth - Uses SNMP v3 with <i>no authentication</i> and <i>no privacy</i></li> <li>priv - Uses SNMP v3 with authentication and privacy</li> </ul> </li> </ul> <p>SNMP inform messages are not supported on SNMP v1.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| udp-port <1-65535>                            | <p>Optional. After specifying the SNMP version, optionally specify the host UDP port</p> <ul style="list-style-type: none"> <li>&lt;1-65535&gt; - Specify the UDP port. The default is 162.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

```
snmp-server {location <WORD>}
```

|                               |                                                                                                                                                                                                                                                                                          |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| snmp-server {location <WORD>} | <p>Configures SNMP-server related settings</p> <ul style="list-style-type: none"> <li>location - Optional. Configures the EX3500's location string <ul style="list-style-type: none"> <li>&lt;WORD&gt; - Specify the location (should not exceed 255 characters).</li> </ul> </li> </ul> |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
snmp-server {notify-filter <WORD> remote <IP>}
```

|                                     |                                                                                                                                                                                                                                                                     |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| snmp-server notify-filter<br><WORD> | Configures SNMP-server related settings <ul style="list-style-type: none"> <li>notify-filter - Optional. Modifies the SNMP server's notify filter <ul style="list-style-type: none"> <li>&lt;WORD&gt; - Specify the SNMP notify-filter name.</li> </ul> </li> </ul> |
| remote <IP>                         | Optional. Configures the remote host's IP address <ul style="list-style-type: none"> <li>&lt;IP&gt; - Specify the IP address in the A.B.C.D format.</li> </ul>                                                                                                      |

```
snmp-server {user <USER-NAME> <GROUP-NAME> remote <IP> v3 {auth/encrypted auth}
[md5/sha] <WORD> {priv [3des/aes128/aes192/aes256/des56] <WORD>}}
```

|                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| snmp-server user <USER-NAME> <GROUP-NAME>                                              | Configures SNMP-server related settings <ul style="list-style-type: none"> <li>user - Optional. Configures the name of the SNMP user (connecting to the SNMP agent) and adds the user to an existing SNMP group. It also specifies the SNMP version type used. In case of SNMP version 3, this command also configures the remote host's IP address and the authentication type used. <ul style="list-style-type: none"> <li>&lt;USER-NAME&gt; - Specify the user's name (should not exceed 32 characters).</li> <li>&lt;GROUP-NAME&gt; - Specify the SNMP group name to which this user is assigned.</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| remote <IP> v3                                                                         | Configures the remote host on which the SNMPv3 engine is running <ul style="list-style-type: none"> <li>&lt;IP&gt; - Specify the remote host's IP address.</li> </ul> <p>This option is available only for SNMPv3 engine.<br/>After configuring the remote host, optionally configure the authentication type and the corresponding authentication password used.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| {auth/encrypted auth} [md5 sha] <WORD> {priv [3des aes128 aes192 aes256 des56] <WORD>} | Optional. Configures authentication and encryption settings <ul style="list-style-type: none"> <li>auth - Specifies the authentication type used and configures the authentication password</li> <li>encrypted - Enables encryption. When enabled all communications between the user and the SNMP engine are encrypted. After enabling encryption, specify the authentication type and configure the authentication password.</li> </ul> <p>The following parameters are common to the 'auth' and 'encrypted' keywords:</p> <ul style="list-style-type: none"> <li>md5 - Uses MD5 to authenticate the user</li> <li>sha - Uses SHA to authenticate the user</li> </ul> <p>The following parameter is common to the 'md5' and 'sha' keywords:</p> <ul style="list-style-type: none"> <li>&lt;WORD&gt; - Specify the authentication password.</li> </ul> <p>If the 'encrypted' option is not being used, enter an 8 - 40 characters ASCII password. Whereas, in case of an encrypted password enter a HEX characters password of 32 characters.</p> <ul style="list-style-type: none"> <li>priv - Optional. Uses SNMPv3 with privacy. Select one of the privacy options: des, aes128, aes192, aes256, des56 <ul style="list-style-type: none"> <li>&lt;WORD&gt; - Configures the privacy password. If the 'encrypted' option is not being used, enter an 8 - 40 characters long ASCII password. Whereas, the encrypted password should be 32 HEX characters.</li> </ul> </li> </ul> |

```
snmp-server {user <USER-NAME> <GROUP-NAME> [v1/v2c/v3]}
```

|                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>snmp-server {user &lt;USER-NAME&gt; &lt;GROUP-NAME&gt; [v1 v2c v3]}</pre> | <p>Configures SNMP-server related settings</p> <ul style="list-style-type: none"> <li>• user – Optional. Configures the name of the SNMP user (connecting to the SNMP agent) and adds the user to an existing SNMP group. It also specifies the SNMP version type used. In case of SNMPv3, this command also configures the authentication type used and the enables encryption.</li> <li>• &lt;USER-NAME&gt; – Specify the user's name (should not exceed 32 characters).</li> <li>• &lt;GROUP-NAME&gt; – Specify the SNMP group name to which this user is assigned.</li> <li>• [v1 v2c v3] – After specifying the group name, specify the SNMP version used. The options are SNMP version v1, SNMP version 2c, and SNMP version 3.</li> </ul> <p>If using SNMP version 3, optionally specify the authentication type and the corresponding authentication password used. Please see previous table for SNMPv3 authentication and encryption configuration details.</p> |
|--------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
snmp-server {view <VIEW-NAME> <OID-TREE-STRING> [excluded|included]}
```

|                                                        |                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>snmp-server view &lt;VIEW-NAME&gt;</pre>          | <p>Configures SNMP-server related settings</p> <ul style="list-style-type: none"> <li>• view – Optional. Creates an SNMP view. SNMP views are used to control user access to the MIB.</li> <li>• &lt;VIEW-NAME&gt; – Provide a name for this SNMP view (should not exceed 32 characters).</li> </ul> |
| <pre>&lt;OID-TREE-STRING&gt; [excluded included]</pre> | <p>Configures the OID (object identifier) of a branch within the MIB tree</p> <ul style="list-style-type: none"> <li>• excluded – Specifies an excluded view</li> <li>• included – Specifies an included view</li> </ul>                                                                             |

### Examples

```
nx9500-6C8809(config-ex3500-management-policy-test)#snmp-server enable traps
nx9500-6C8809(config-ex3500-management-policy-test)#snmp-server host 192.168.13.10
snmp-teststring version 1 udp-port 170
nx9500-6C8809(config-ex3500-management-policy-test)#snmp-server host 1.2.3.4 inform
retry 2 test version 3 auth udp-port 180
nx9500-6C8809(config-ex3500-management-policy-test)#snmp-server engine-id local
1234567890
nx9500-6C8809(config-ex3500-management-policy-test)#show context
ex3500-management-policy test
 http secure-server
 enable password level 3 7 12345678901020304050607080929291
 snmp-server enable traps authentication
 snmp-server notify-filter 3 remote 1.2.3.4
 snmp-server notify-filter 1 remote 127.0.0.1
 snmp-server notify-filter 2 remote 192.168.13.10
 snmp-server host 1.2.3.4 inform timeout 1500 retry 2 test version 3 auth udp-port 180
 snmp-server host 192.168.13.10 snmp-teststring version 1 udp-port 170
 snmp-server engine-id local 1234567890
 memory falling-threshold 50
 memory rising-threshold 95
 process-cpu falling-threshold 60
 process-cpu rising-threshold 80
nx9500-6C8809(config-ex3500-management-policy-test)#
```

### Related Commands

|           |                                                                 |
|-----------|-----------------------------------------------------------------|
| <b>no</b> | Removes SNMP server related settings or reverts them to default |
|-----------|-----------------------------------------------------------------|

ssh

Configures the SSH server settings used to authenticate SSH connection to a EX3500 switch

Management access to an EX3500 switch can be enabled/disabled as required using separate interfaces and protocols (HTTP, SSH). Disabling unused and insecure interfaces and unused management services can dramatically reduce an attack footprint and free resources within an EX3500 management policy.

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 7510

#### Syntax

```
ssh [authentication-retries <1-5>|server|server-key size <512-1024>|timeout <1-120>]
```

#### Parameters

```
ssh [authentication-retries <1-5>|server|server-key size <512-1024>|timeout <1-120>]
```

|                              |                                                                                                                                                                                                                                                                                                                          |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ssh                          | Enables SSH management access to an EX3500 switch. This option is disabled by default. Use this command to configure SSH access settings.                                                                                                                                                                                |
| authentication-retries <1-5> | Configures the maximum number of retries made to connect to the SSH server resource <ul style="list-style-type: none"><li>• &lt;1-5&gt; – Specify a value from 1 - 5. The default setting is 3.</li></ul>                                                                                                                |
| server                       | Enables SSH server connection                                                                                                                                                                                                                                                                                            |
| server-key size <512-1024>   | Configures the SSH server key size <ul style="list-style-type: none"><li>• &lt;512-1024&gt; – Specify the SSH server key from 512 - 1,024. The default length is 768.</li></ul>                                                                                                                                          |
| timeout <1-120>              | Configures the SSH server resource inactivity timeout value in seconds. When the specified time is exceeded, the SSH server resource becomes unreachable and must be re-authenticated. <ul style="list-style-type: none"><li>• &lt;1-120&gt; – Specify a value from 1 120 seconds. The default is 120 seconds.</li></ul> |

#### Examples

```
nx9500-6C8809(config-ex3500-management-policy-test)#ssh authentication-retries 4
nx9500-6C8809(config-ex3500-management-policy-test)#ssh timeout 90
nx9500-6C8809(config-ex3500-management-policy-test)#ssh server-key size 600
nx9500-6C8809(config-ex3500-management-policy-test)#ssh server
nx9500-6C8809(config-ex3500-management-policy-test)#show context
ex3500-management-policy test
 ssh server
 ssh authentication-retries 4
 ssh timeout 90
 ssh server-key size 600
 http secure-server
 enable password level 3 7 12345678901020304050607080929291
 snmp-server enable traps authentication
 --More--
nx9500-6C8809(config-ex3500-management-policy-test)#
```

#### Related Commands

|    |                                                    |
|----|----------------------------------------------------|
| no | Disables SSH management access to an EX3500 switch |
|----|----------------------------------------------------|

username

Configures a EX3500 switch user settings

The EX3500 switch user details are stored in a local database on the NX 95XX, NX 7510, or WiNG VM. You can configure multiple users, each having a unique name, access level, and password.

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 7510

#### Syntax

```
username <USER-NAME> [access-level <0-15>|nopassword|password [0|7] <PASSWORD>]
```

#### Parameters

```
username <USER-NAME> [access-level <0-15>|nopassword|password [0|7] <PASSWORD>]
```

|                              |                                                                                                                                                                                                                                                                                                           |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| username <USER-NAME>         | Configures the TACACS server port username <ul style="list-style-type: none"><li>• &lt;USER-NAME&gt; - Specify the user name (should not exceed 32 characters)</li></ul>                                                                                                                                  |
| access-level <0-15>          | Configures the access level for this user. This value determines the access priority of each user requesting access and interoperability with EX3500 switch. <ul style="list-style-type: none"><li>• &lt;0-15&gt; - Specify the access level from 0 - 15. The default is 0.</li></ul>                     |
| nopassword                   | Allows user to login without a password                                                                                                                                                                                                                                                                   |
| password [0 7]<br><PASSWORD> | Configures the password for this user <ul style="list-style-type: none"><li>• 0 - Configures a plain text password</li><li>• 7 - Configures an encrypted password (should be 32 characters in length)<ul style="list-style-type: none"><li>• &lt;PASSWORD&gt; - Specify the password.</li></ul></li></ul> |

#### Examples

```
nx9500-6C8809(config-ex3500-management-policy-test)#username user1 access-level 5
nx9500-6C8809(config-ex3500-management-policy-test)#username user1 password 0 user1@1234
nx9500-6C8809(config-ex3500-management-policy-test)#show context
ex3500-management-policy test
ssh server
ssh authentication-retries 4
ssh timeout 90
ssh server-key size 600
http secure-server
enable password level 3 7 12345678901020304050607080929291
username user1 access-level 5
username user1 password 7 5c4786c1e52f913d38168ce89154a079
snmp-server enable traps authentication
snmp-server notify-filter 3 remote 1.2.3.4
snmp-server notify-filter 1 remote 127.0.0.1
--More--
nx9500-6C8809(config-ex3500-management-policy-test)#
```

#### Related Commands

|    |                                 |
|----|---------------------------------|
| no | Removes this SNMP user settings |
|----|---------------------------------|

no (ex3500-management-policy-config-mode)

Removes or reverts this EX3500 management policy settings

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 7510

## Syntax

```
no [enable|http|memory|process-cpu|snmp-server|ssh|username]
no enable password {level <0-15>}
no http [port|secure-port|secure-sever|server]
no memory [falling-threshold|rising-threshold]
no process-cpu [falling-threshold|rising-threshold]
no snmp-server {community/contact/enable/engine-id/group/host/location/
notify-filter/user/view}
no snmp-server {community <STRING>}
no snmp-server {contact}
no snmp-server {enable traps {authentication/link-up-down}}
no snmp-server {engine-id [local/remote <IP>]}
no snmp-server {group <GROUP-NAME> [v1/v2c/v3 [auth/noauth/priv]]}
no snmp-server {location}
no snmp-server {notify-filter <WORD> remote <IP>}
no snmp-server {user <USER-NAME> [v1/v2c/v3]}
no snmp-server {user <USER-NAME> <GROUP-NAME> remote-host <IP> v3}
no snmp-server {view <VIEW-NAME> {<OID-TREE-STRING>}}
no ssh [authentication-retries|server|server-key size <512-1024>|timeout]
no username
no snmp-server {host <IP>}
```

## Parameters

no <PARAMETERS>

|                 |                                                                               |
|-----------------|-------------------------------------------------------------------------------|
| no <PARAMETERS> | Removes this EX3500 management policy settings based on the parameters passed |
|-----------------|-------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-ex3500-management-policy-test)#show context
ex3500-management-policy test
 ssh server
 ssh authentication-retries 4
 ssh timeout 90
 ssh server-key size 600
 http secure-server
 enable password level 3 7 12345678901020304050607080929291
 username user1 access-level 5
 username user1 password 7 5c4786c1e52f913d38168ce89154a079
 snmp-server enable traps authentication
 snmp-server notify-filter 3 remote 1.2.3.4
 snmp-server notify-filter 1 remote 127.0.0.1
 snmp-server notify-filter 2 remote 192.168.13.10
 snmp-server host 1.2.3.4 inform timeout 1500 retry 2 test version 3 auth udp-port 180
 snmp-server host 192.168.13.10 snmp-test-string version 1 udp-port 170
 snmp-server engine-id local 1234567890
 memory falling-threshold 50
 memory rising-threshold 95
 process-cpu falling-threshold 60
 process-cpu rising-threshold 80
nx9500-6C8809(config-ex3500-management-policy-test)#
nx9500-6C8809(config-ex3500-management-policy-test)#no http secure-server
nx9500-6C8809(config-ex3500-management-policy-test)#no memory falling-threshold
nx9500-6C8809(config-ex3500-management-policy-test)#no process-cpu rising-threshold
nx9500-6C8809(config-ex3500-management-policy-test)#no snmp-server notify-filter 3 remote
1.2.3.4
nx9500-6C8809(config-ex3500-management-policy-test)#show context
ex3500-management-policy test
 ssh server
 ssh authentication-retries 4
 ssh timeout 90
 ssh server-key size 600
 enable password level 3 7 12345678901020304050607080929291
 username user1 access-level 5
```

```

username user1 password 7 5c4786c1e52f913d38168ce89154a079
snmp-server enable traps authentication
snmp-server notify-filter 1 remote 127.0.0.1
snmp-server notify-filter 2 remote 192.168.13.10
snmp-server host 1.2.3.4 inform timeout 1500 retry 2 test version 3 auth udp-port 180
snmp-server host 192.168.13.10 snmp-test-string version 1 udp-port 170
snmp-server engine-id local 1234567890
memory rising-threshold 95
process-cpu falling-threshold 60
nx9500-6C8809(config-ex3500-management-policy-test)#

```

### *ex3500-qos-class-map-policy*

Creates a EX3500 QoS (Quality of Service) class map policy and enters its configuration mode

A QoS class map policy contains a set of DiffServ (Differentiated Services) classification criteria that are used to classify incoming traffic into different category and provide differentiated service based on this classification. Each policy defines a set match criteria rules that use objects, such as access lists, IP precedence or DSCP values, and VLANs. When configured and applied, the policy classifies traffic based on layer 2, layer 3, or layer 4 information contained in each incoming packet.

#### **Supported in the following platforms:**

- Service Platforms — NX 95XX, NX 7510

#### **Syntax**

```
ex3500-qos-class-map-policy <POLICY-NAME>
```

#### **Parameters**

```
ex3500-qos-class-map-policy <POLICY-NAME>
```

|                            |                                                                                            |
|----------------------------|--------------------------------------------------------------------------------------------|
| <b>&lt;POLICY-NAME&gt;</b> | Specify the EX3500 QoS class map policy name. If the policy does not exist, it is created. |
|----------------------------|--------------------------------------------------------------------------------------------|

#### **Examples**

```

nx9500-6C8809(config)#ex3500-qos-class-map-policy dscp
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#?
EX3500_Qos_class_map Mode commands:
 description Class-map description
 match Defines the match criteria to classify traffic
 no Negate a command or set its defaults
 rename Redefines the name of class-map

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#

```

## Related Commands

Removes an existing EX3500 QoS class map policy

## ex3500-qos-class-map-policy config commands

The following table summarizes EX3500 QoS class map policy configuration mode commands:

**Table 20: EX3500 QoS Class Map Policy Config Commands**

| Command                                 | Description                                                               |
|-----------------------------------------|---------------------------------------------------------------------------|
| <a href="#">description</a> on page 412 | Configures a description for this EX3500 QoS class map policy             |
| <a href="#">match</a> on page 412       | Configures match criteria rules used to classify traffic                  |
| <a href="#">rename</a> on page 414      | Renames an existing EX3500 QoS class map object                           |
| <a href="#">no</a> on page 415          | Removes this EX3500 QoS class map policy's description and match criteria |

### description

Configures this EX3500 QoS class map policy's description

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 7510

#### Syntax

```
description <LINE>
```

#### Parameters

```
description <LINE>
```

|                    |                                                                                                                                                                                                                                                                     |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| description <LINE> | Configures this EX3500 QoS class map policy's description <ul style="list-style-type: none"><li>• &lt;LINE&gt; - Enter a description that allows to you differentiate it from other policies with similar configuration (should not exceed 64 characters)</li></ul> |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#description "Matches packets marked
for DSCP service 3"
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#show context
ex3500-qos-class-map-policy dscp
 description "Matches packets marked for DSCP service 3"
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#
```

#### Related Commands

|                    |                                                        |
|--------------------|--------------------------------------------------------|
| <a href="#">no</a> | Removes this EX3500 QoS class map policy's description |
|--------------------|--------------------------------------------------------|

### match

Configures match criteria rules used to classify traffic

Access lists, IP precedence, DSCP values, or VLANs are commonly used to classify traffic. Access lists select traffic based on layer 2, layer 3, or layer 4 information contained in each packet.

Supported in the following platforms:



- Service Platforms — NX 95XX, NX 7510

### Syntax

```
match [access-list [ex3500-ext-access-list|ex3500-std-access-list|mac-acl]
<ACL-NAME>|cos <0-7>|ip [dscp <0-63>|precedence <0-7>]|ipv6 dscp <0-63>|vlan <1-4094>]
```

### Parameters

```
match [access-list [ex3500-ext-access-list|ex3500-std-access-list|mac-acl]
<ACL-NAME>|cos <0-7>|ip [dscp <0-63>|precedence <0-7>]|ipv6 dscp <0-63>|vlan <1-4094>]
```

|                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| match                                                                           | <p>Configures the match criteria.</p> <p>The options are: access-list, cos, ip, ipv6, vlan Incoming packets matching the specified criteria are included in this QoS class map.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| access-list [ex3500-ext-access-list ex3500-std-access-list  mac-acl] <ACL-NAME> | <p>Uses access lists to provide the match criteria. You can use any one the following ACL types to classify traffic:</p> <ul style="list-style-type: none"> <li>• ex3500-ext-access-list - Uses an IPv4 EX3500 extended ACL</li> <li>• ex3500-std-access-list - Uses an IPv4 EX3500 standard ACL</li> <li>• mac-acl - Uses a MAC EX3500 ACL</li> </ul> <p>The following keyword is common to all of the above ACL types:</p> <ul style="list-style-type: none"> <li>• &lt;ACL-NAME&gt; - Specify the ACL name (should be existing and configured).</li> </ul>                                                                                                                                                                                                                                                                                                                                     |
| cos <0-7>                                                                       | <p>Configures the CoS (class of service) value used to apply user priority. CoS is a form of QoS applicable only to layer 2 Ethernet frames. It uses 3-bits (8 values) of the 802.1Q tag to differentiate and shape network traffic.</p> <ul style="list-style-type: none"> <li>• &lt;0-7&gt; - Specify the CoS value from 0 - 7.</li> </ul> <p>Following are the 8 traffic classes based on the CoS value:</p> <ul style="list-style-type: none"> <li>• 000 (0) - Routine</li> <li>• 001 (1) - Priority</li> <li>• 010 (2) - Immediate</li> <li>• 011 (3) - Flash</li> <li>• 100 (4) - Flash Override</li> <li>• 101 (5) - Critical</li> <li>• 110 (6) - Internetwork Control</li> <li>• 111 (7) - Network Control</li> </ul>                                                                                                                                                                    |
| ip [dscp <0-63>] precedence <0-7>]                                              | <p>Configures the IPv4 DSCP value to match and/or the IP precedence value to match.</p> <ul style="list-style-type: none"> <li>• &lt;0-63&gt; - Specify the DSCP value from 0 - 63. Use this option to specify the ToS (type of service) field values included in the IP header. The ToS field exists between the header length and the total length fields. The DSCP constitutes the first 6 bits of the ToS field.</li> <li>• precedence &lt;0-7&gt; - Configures the IP precedence to match. Following are the 8 traffic classes based on the IP precedence values: <ul style="list-style-type: none"> <li>• 000 (0) - Routine</li> <li>• 001 (1) - Priority</li> <li>• 010 (2) - Immediate</li> <li>• 011 (3) - Flash</li> <li>• 100 (4) - Flash Override</li> <li>• 101 (5) - Critical</li> <li>• 110 (6) - Internetwork Control</li> <li>• 111 (7) - Network Control</li> </ul> </li> </ul> |

|                  |                                                                                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| ipv6 dscp <0-63> | Configures the IPv6 DSCP value to match <ul style="list-style-type: none"> <li>• &lt;0-63&gt; - Specify the DSCP value from 0 - 63.</li> </ul> |
| vlan <1-4094>    | Configures the VLAN to match <ul style="list-style-type: none"> <li>• &lt;1-4094&gt; - Specify the VLAN ID.</li> </ul>                         |

Usage Guidelines

When configuring match entries, take into consideration the following points:

- Deny rules included in an ACL (associated with a EX3500 QoS class map policy) are ignored whenever an incoming packet matches the ACL.
- A class map policy cannot include both IP ACL or IP precedence rule and a VLAN rule.
- A class map policy containing a MAC ACL or VLAN rule cannot include either an IP ACL or a IP precedence rule.
- A class map policy can include a maximum of 16 match entries.

Examples

```

nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#match ip dscp 3
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#show context
ex3500-qos-class-map-policy dscp
 description "Matches packets marked for DSCP service 3"
 match ip dscp 3
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#
nx9500-6C8809(config-ex3500-qos-class-map-policy-test2)#match ip precedence 1

```

Related Commands

|    |                                                                              |
|----|------------------------------------------------------------------------------|
| no | Removes match criteria rules configured for this EX3500 QoS class map policy |
|----|------------------------------------------------------------------------------|

rename

Renames an existing EX3500 QoS class map policy

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 7510

Syntax

```
rename <EX3500-QOS-CLASS-MAP-POLICY-NAME> <NEW-EX3500-QOS-CLASS-MAP-POLICY-NAME>
```

Parameters

```
rename <EX3500-QOS-CLASS-MAP-POLICY-NAME> <NEW-EX3500-QOS-CLASS-MAP-POLICY-NAME>
```

|                                                                                  |                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| rename <EX3500-QOS-CLASS-MAP-POLICY-NAME> <NEW-EX3500-QOS-CLASS-MAP-POLICY-NAME> | Renames an existing EX3500 QoS class map <ul style="list-style-type: none"> <li>• &lt;EX3500-QOS-CLASS-MAP-POLICY-NAME&gt; - Enter the EX3500 QoS class map's current name.</li> <li>• &lt;NEW-EX3500-QOS-CLASS-MAP-POLICY-NAME&gt; - Enter the new name.</li> </ul> |
|----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Examples

```

nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#rename [TAB]
dscp test test2
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#rename test2 IP_Precedence
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#rename [TAB]
dscp IP_Precedence test
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#

```



no

description

Removes this EX3500 QoS class map policy's description and match criteria

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 7510

Syntax

```
no [description|match]
no description
no match [access-list [ex3500-ext-access-list|ex3500-std-access-list|mac-acl]
<ACL-NAME>|cos <0-7>|ip [dscp <0-63>|precedence <0-7>]|ipv6 dscp <0-63>|vlan <1-4094>]
```

Parameters

```
no <PARAMETERS>
```

|                 |                                                                                   |
|-----------------|-----------------------------------------------------------------------------------|
| no <PARAMETERS> | Removes the EX3500 QoS class map policy's settings based on the parameters passed |
|-----------------|-----------------------------------------------------------------------------------|

Examples

The following example shows the EX3500 QoS class map policy 'test' settings before the 'no' command are executed:

```
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#show context
ex3500-qos-class-map-policy dscp
 description "Matches packets marked for DSCP service 3"
 match ip dscp 3
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#no description
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#no match ip dscp
```

The following example shows the EX3500 QoS class map policy 'test' settings after the 'no' command are executed:

```
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#show context
ex3500-qos-class-map-policy test
nx9500-6C8809(config-ex3500-qos-class-map-policy-dscp)#
```

### *ex3500-qos-policy-map*

Creates an EX3500 policy map and enters its configuration mode

An EX3500 policy map contains one or more EX3500 QoS class maps traffic classifications (existing and configured) and can be attached to multiple interfaces. Creates an EX3500 policy map, and then use the class parameter to configure policies for traffic that matches the criteria defined in the EX3500 QoS class map policy. For more information, see [match](#).

**Supported in the following platforms:**

- Service Platforms — NX 95XX, NX 7510

**Syntax**

```
ex3500-qos-policy-map <EX3500-QOS-POLICY-MAP-NAME>
```

**Parameters**

```
ex3500-qos-policy-map <EX3500-QOS-POLICY-MAP-NAME>
```

```
<EX3500-QOS-POLICY-MAP-NAME> Specify the EX3500 policy map's name
```

### Examples

```
nx9500-6C8809(config)#ex3500-qos-policy-map testPolicyMap
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap)#?
EX3500_Qos_policy_map Mode commands:
 class Defines a traffic classification for the policy
 description Policy-map description
 no Negate a command or set its defaults

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap)#
```

### Related Commands

```
no Removes an existing EX3500 QoS policy map
```

## ex3500-qos-policy-map config commands

The following table summarizes EX3500 QoS policy map configuration mode commands:

**Table 21: EX3500 QoS Policy Map Config Commands**

| Command                              | Description                                                                                                                                               |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>class</code> on page 416       | Creates a policy map class and enters its configuration mode                                                                                              |
| <code>description</code> on page 424 | Configures this EX3500 QoS policy map's description                                                                                                       |
| <code>no</code> on page 425          | Removes this EX3500 QoS policy map's settings. Use this keyword to remove or modify the description and to remove the QoS traffic classification created. |

### class

Creates a policy map class and enters its configuration mode. The policy map class is a traffic classification upon which a policy can act.

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 7510

#### Syntax

```
class <EX3500-QoS-CLASS-MAP-POLICY-NAME>
```

#### Parameters

```
class <EX3500-QoS-CLASS-MAP-POLICY-NAME>
```

|                                          |                                                                                    |
|------------------------------------------|------------------------------------------------------------------------------------|
| class <EX3500-QoS-CLASS-MAP-POLICY-NAME> | Specify the EX3500 QoS class map policy's name (should be existing and configured) |
|------------------------------------------|------------------------------------------------------------------------------------|

### Examples

```

nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap)#class dscp
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#?
commands:
 no Negate a command or set its defaults
 police Defines a policer for classified traffic
 set Classify IP traffic

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#

```

### Related Commands

|                                                   |                                                                                     |
|---------------------------------------------------|-------------------------------------------------------------------------------------|
| <b>no</b> on page 425 (global config mode)        | Removes this EX3500 QoS policy map class association                                |
| <b>set</b> on page 422                            | Sets CoS value, PHB (per-hop behavior) value, and IP DSCP value in matching packets |
| <b>police</b> on page 417                         | Configures an enforcer for classified traffic                                       |
| <b>no</b> on page 424(ex3500 qos policy map mode) | Removes this traffic classification's settings                                      |

### police

Configures an enforcer for classified traffic

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 7510

#### Syntax

```

police [flow|srtcm-color-aware|srtcm-color-blind|trtcm-color-aware|trtcm-color-blind]
police flow <0-1000000> <0-16000000> conform-action transmit violate-action [<0-63>|drop]
police [srtcm-color-aware|srtcm-color-blind] <0-1000000> <0-16000000>
<0-16000000> conform-action transmit exceed-action [<0-63>|drop] violate-action [<0-63>|
drop]
police [trtcm-color-aware|trtcm-color-blind] <0-1000000> <0-16000000> <0-1000000>
<0-16000000>
conform-action transmit exceed-action [<0-63>|drop] violate-action [<0-63>|drop]

```

#### Parameters

```

police flow <0-1000000> <0-16000000> conform-action transmit violate-action [<0-63>|drop]

```

|                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| police                           | Configures an enforcer for classified traffic                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| flow <0-1000000><br><0-16000000> | <p>Configures an enforcer for classified traffic based on the metered flow rate</p> <ul style="list-style-type: none"> <li>• &lt;0-1000000&gt; - Configures the CIR (committed information rate) from 0 -1000000 kilobits per second.</li> <li>• &lt;0-16000000&gt; - Configures the BC (committed burst size) from 0 - 16000000 bytes.</li> </ul> <p>Policing is based on a token bucket, where bucket depth (i.e., the maximum burst before the bucket overflows) is specified by the committed-burst field, and the average rate tokens are added to the bucket is specified by the committed-rate option. Note, the token bucket functions similar to that described in RFC 2697 and RFC 2698.</p> <p>The behavior of the meter is specified in terms of one <i>token bucket</i> (C), the rate at which the tokens are incremented CIR and the maximum size of the token bucket BC.</p> <p>The token bucket C is initially full, that is, the token count <math>T_c(0) = BC</math>. Thereafter, the token count <math>T_c</math> is updated CIR times per second as follows: The token bucket C is initially full, that is, the token count <math>T_c(0) = BC</math>. Thereafter, the token count <math>T_c</math> is updated CIR times per second as follows:</p> |
| conform-action transmit          | <p>Configures the action applied when packets fall within the specified CIR and BC limits</p> <ul style="list-style-type: none"> <li>• transmit - Transmits packets falling within the specified CIR and BC limits. This is subject to there being enough tokens to service the packet, in which case the packet is set green.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| violate-action [<0-63> drop]     | <p>Configures the action applied when packets violate the specified CIR and BC limits</p> <ul style="list-style-type: none"> <li>• &lt;0-63&gt; - Applies a new DSCP value. Select the DSCP value from 0 - 63.</li> <li>• drops - Drops packets violating the specified CIR and BC limits</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

```
police [srtcm-color-aware|srtcm-color-blind] <0-1000000> <0-16000000> <0-16000000>
conform-action transmit exceed-action [<0-63>|drop] violate-action [<0-63>|drop]
```

|                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| police                                                                       | Configures an enforcer for classified traffic                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| [srtcm-color-aware  srtcm-color-blind] <0-1000000> <0-16000000> <0-16000000> | <p>Configures an enforcer for classified traffic based on single rate three color meter (srTCM) mode. The srTCM as defined in RFC 2697 meters a traffic stream and processes its packets according to three traffic parameters – CIR, BC, and BE (Excess Burst Size).</p> <ul style="list-style-type: none"> <li>• srtcm-color-blind - Single rate three color meter in color-blind mode</li> <li>• srtcm-color-aware - Single rate three color meter in color-aware mode</li> </ul> <p>The meter operates in one of two modes. In the color-blind mode, the meter assumes that the packet stream is uncolored. In color-aware mode the meter assumes that some preceding entity has pre-colored the incoming packet stream so that each packet is either green, yellow, or red. The marker (re)colors an IP packet according to the results of the meter. The color is coded in the DS field [RFC 2474] of the packet.</p> <ul style="list-style-type: none"> <li>• &lt;0-1000000&gt; – Configures the CIR from 0 -1000000 kilobits per second. <ul style="list-style-type: none"> <li>• &lt;0-16000000&gt; – Configures the BC from 0 - 1600000 bytes.</li> <li>• &lt;0-16000000&gt; – Configures the BE from 0 - 1600000 bytes.</li> </ul> </li> </ul> <p>The behavior of the meter is specified in terms of its mode and two token buckets, C and E, which both share the common rate CIR. The maximum size of the token bucket C is BC and the maximum size of the token bucket E is BE. The token buckets C and E are initially full, that is, the token count <math>T_c(0) = BC</math> and the token count <math>T_e(0) = BE</math>. Thereafter, the token counts <math>T_c</math> and <math>T_e</math> are updated CIR times per second as follows:</p> <ul style="list-style-type: none"> <li>• If <math>T_c</math> is less than BC, <math>T_c</math> is incremented by one, else</li> <li>• If <math>T_e</math> is less than BE, <math>T_e</math> is incremented by one, else</li> <li>• neither <math>T_c</math> nor <math>T_e</math> is incremented.</li> </ul> <p>When a packet of size B bytes arrives at time t, the following happens if srTCM is configured to operate in color-blind mode:</p> <ul style="list-style-type: none"> <li>• If <math>T_c(t)-B &gt; 0</math>, the packet is green and <math>T_c</math> is decremented by B down to the minimum value of 0, else</li> <li>• if <math>T_e(t)-B &gt; 0</math>, the packets is yellow and <math>T_e</math> is decremented by B down to the minimum value of 0,</li> <li>• else the packet is red and neither <math>T_c</math> nor <math>T_e</math> is decremented.</li> </ul> <p>When a packet of size B bytes arrives at time t, the following happens if srTCM is configured to operate in color-aware mode:</p> <ul style="list-style-type: none"> <li>• If the packet has been pre-colored as green and <math>T_c(t)-B &gt; 0</math>, the packet is green and <math>T_c</math> is decremented by B down to the minimum value of 0, else</li> <li>• If the packet has been pre-colored as yellow or green and if</li> <li>• <math>T_e(t)-B &gt; 0</math>, the packets is yellow and <math>T_e</math> is decremented by B down to the minimum value of 0, else the packet is red and neither <math>T_c</math> nor <math>T_e</math> is decremented.</li> </ul> <p>The metering policy guarantees a deterministic behavior where the volume of green packets is never smaller than what has been determined by the CIR and BC, that is, tokens of a given color are always spent on packets of that color. Refer to RFC 2697 for more information on other aspects of srTCM.</p> |
| conform-action transmit                                                      | <p>Configures the action applied when packet rates fall within the specified CIR and BC limits</p> <ul style="list-style-type: none"> <li>• transmit – Transmits packets falling within the specified CIR and BC limits</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

|                              |                                                                                                                                                                                                                                                                                                         |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| exceed-action [<0-63> drop]  | <p>Configures the action applied when packet rates exceed the specified CIR and BC limits</p> <ul style="list-style-type: none"> <li>• &lt;0-63&gt; - Applies a new DSCP value. Select the DSCP value from 0 - 63</li> <li>• drops - Drops packets exceeding the specified CIR and BC limits</li> </ul> |
| violate-action [<0-63> drop] | <p>Configures the action applied when packet rates exceed the specified BE limit</p> <ul style="list-style-type: none"> <li>• &lt;0-63&gt; - Applies a new DSCP value. Select the DSCP value from 0 - 63</li> <li>• drops - Drops packets exceeding the specified BE limit</li> </ul>                   |

```

police [trtcm-color-aware|trtcm-color-blind] <0-1000000> <0-16000000> <0-1000000>
<0-16000000> conform-action transmit exceed-action [<0-63>|drop] violate-action [<0-63>|
drop]

```



|                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| police                                                                                  | Configures an enforcer for classified traffic                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| [trtcm-color-aware] trtcm-color-blind <0-1000000> <0-16000000> <0-1000000> <0-16000000> | <p>Configures an enforcer for classified traffic based on a two rate three color meter (trTCM) mode. The trTCM as defined in RFC 2698 meters a traffic stream and processes its packets based on two rates – CIR and PIR (Peak Information Rate), and their associated burst sizes - BC and BP (Peak Burst Size).</p> <ul style="list-style-type: none"> <li>• trtcm-color-blind - Two rate three color meter in color-blind mode</li> <li>• trtcm-color-aware - Two rate three color meter in color-aware mode <ul style="list-style-type: none"> <li>• &lt;0-1000000&gt; - Configures the CIR from 0 - 1000000 kilobits per second</li> <li>• &lt;0-16000000&gt; - Configures the BC from 0 - 16000000 bytes.</li> <li>• &lt;0-1000000&gt; - Configures the PIR from 0 - 1000000 kilobits per second</li> <li>• &lt;0-16000000&gt; - Configures the BP from 0 - 16000000 bytes</li> </ul> </li> </ul> <p>The meter operates in one of two modes. In the color-blind mode, the meter assumes that the packet stream is uncolored. In color-aware mode the meter assumes that some preceding entity has pre-colored the incoming packet stream so that each packet is either green, yellow, or red. The marker (re)colors an IP packet according to the results of the meter. The color is coded in the DS field [RFC 2474] of the packet.</p> <p>The behavior of the meter is specified in terms of its mode and two token buckets, P and C, which are based on the rates PIR and CIR, respectively. The maximum size of the token bucket P is BP and the maximum size of the token bucket C is BC. The token buckets P and C are initially (at time 0) full, that is, the token count <math>T_p(0) = BP</math> and the token count <math>T_c(0) = BC</math>. Thereafter, the token count <math>T_p</math> is incremented by one PIR times per second up to BP and the token count <math>T_c</math> is incremented by one CIR times per second up to BC.</p> <p>When a packet of size B bytes arrives at time t, the following happens if trTCM is configured to operate in color-blind mode:</p> <ul style="list-style-type: none"> <li>• If <math>T_p(t) - B &lt; 0</math>, the packet is red, else</li> <li>• if <math>T_c(t) - B &lt; 0</math>, the packet is yellow and <math>T_p</math> is decremented by B, else</li> <li>• The packet is green and both <math>T_p</math> and <math>T_c</math> are decremented by B.</li> </ul> <p>When a packet of size B bytes arrives at time t, the following happens if trTCM is configured to operate in color-aware mode:</p> <ul style="list-style-type: none"> <li>• If the packet has been pre-colored as red or if <math>T_p(t) - B &lt; 0</math>, the packet is red, else</li> <li>• if the packet has been pre-colored as yellow or if <math>T_c(t) - B &lt; 0</math>, the packet is yellow and <math>T_p</math> is decremented by B, else</li> <li>• the packet is green and both <math>T_p</math> and <math>T_c</math> are decremented by B.</li> </ul> <p>The trTCM can be used to mark a IP packet stream in a service, where different, decreasing levels of assurances (either absolute or relative) are given to packets which are green, yellow, or red. Refer to RFC 2698 for more information on other aspects of trTCM.</p> |
| conform-action transmit                                                                 | <p>Configures the action applied when packet rates fall within the specified CIR and BP limits</p> <ul style="list-style-type: none"> <li>• transmit - Transmits packets falling within the specified CIR and BC limits</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

|                              |                                                                                                                                                                                                                                                                                                                                  |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| exceed-action [<0-63> drop]  | Configures the action applied when packet rates exceed the specified CIR limit, but are within the specified PIR limit <ul style="list-style-type: none"> <li>• &lt;0-63&gt; – Applies a new DSCP value. Select the DSCP value from 0 - 63.</li> <li>• drops – Drops packets exceeding the specified CIR and BC limit</li> </ul> |
| violate-action [<0-63> drop] | Configures the action applied when packet rates exceed the specified PIR limit <ul style="list-style-type: none"> <li>• &lt;0-63&gt; – Applies a new DSCP value. Select the DSCP value from 0 - 63.</li> <li>• drops – Drops packets exceeding the specified BE limi</li> </ul>                                                  |

### Usage Guidelines

When configuring the traffic class enforcer parameters, consider the following factors:

- You can configure up to 200 enforcers/policers (i.e., class maps) for ingress ports.
- The committed-rate cannot exceed the configured interface speed, and the committed-burst cannot exceed 16 Mbytes.

### Examples

The following example uses the **police > trtcm-color-blind** command to limit the average bandwidth to 100,000 Kbps, the committed burst rate to 4000 bytes, the peak information rate to 1,000,000 Kbps, the peak burst size to 6000, to remark any packets exceeding the committed burst size, and to drop any packets exceeding the peak information rate.

```
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#police
 trtcm-color-blind 100000 4000 100000 6000 conform-action transmit exceed-action 0 violate-
action drop
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#show context
 class dscp
 police trtcm-color-blind 100000 4000 100000 6000 conform-action transmit exceed-action 0
violate-action drop
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#
```

### Related Commands

|                       |                                       |
|-----------------------|---------------------------------------|
| <b>no</b> on page 424 | Removes the traffic enforcer settings |
|-----------------------|---------------------------------------|

### set

Sets CoS value, PHB value, and IP DSCP value in matching packets

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 7510

#### Syntax

```
set [cos <0-7>|ip dscp <0-63>|phb <0-7>]
```

#### Parameters

```
set [cos <0-7>|ip dscp <0-63>|phb <0-7>]
```

|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| set            | Sets the match criteria used to identify and classify traffic into different classes. The match criteria options are: CoS, IP DSCP, and PHB values.                                                                                                                                                                                                                                                                                                                                                                                                                             |
| cos <0-7>      | Configures the CoS value for a matching packet (as specified by the match command) in the packet's VLAN tag <ul style="list-style-type: none"> <li>• &lt;0-7&gt; – Specify a value from 0 - 7. The CoS is modified to the value specified here.</li> </ul>                                                                                                                                                                                                                                                                                                                      |
| ip dscp <0-63> | Modifies the IP DSCP value in a matching packet (as specified by the match command) <ul style="list-style-type: none"> <li>• &lt;0-63&gt; – Specify a value from 0 - 63. The DSCP value is modified to the value specified here.</li> </ul>                                                                                                                                                                                                                                                                                                                                     |
| phb <0-7>      | Configures a PHB value for a matching packets <ul style="list-style-type: none"> <li>• &lt;0-7&gt; – Specify a value from 0 - 7.</li> </ul> <p>The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion. A packet is marked green, yellow, or red as per the following:</p> <ul style="list-style-type: none"> <li>• green if it does not exceed the CIR and BC limits</li> <li>• yellow if it exceeds the CIR and BC limits, but not the BE limit, and</li> <li>• red otherwise.</li> </ul> |

## Examples

The following example uses the **set > phb** command to classify the service that incoming packets will receive, and then uses the **police > trtcm-color-blind** command to limit the average bandwidth to 100,000 Kbps, the committed burst rate to 4000 bytes, the peak information rate to 1,000,000 Kbps, the peak burst size to 6000 bytes, to remark any packets exceeding the committed burst size, and to drop any packets exceeding the peak information rate.

```

nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-test2)#set phb 3
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-test2)# police
trtcm-color-blind 100000 4000 1000000 6000 conform-action transmit exceed-action 0 violate-
action drop
nx9500-6C8809nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-
test2)#show
context
class test2
set phb 3
police trtcm-color-blind 100000 4000 100000 6000 conform-action transmit exceed-action 0
violate-action drop
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-test2)#

```

The following example uses the **set > ip dscp** command to classify the service that incoming packets will receive, and then uses the **police > flow** command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4000 bytes, and configure the response to drop any violating packets:

```

nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#set ip dscp 3
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)# police flow
100000 4000
conform-action transmit violate-action drop
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#show context
class dscp
set ip dscp 3
police flow 100000 4000 conform-action transmit violate-action drop
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#

```

## Related Commands

no on page 424

Removes CoS value, PHB value, or IP DSCP value from this traffic class

no

Removes this traffic classification's settings

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 7510

Syntax

```
no [police|set]
no police [flow|srctcm-color-aware|srctcm-color-blind|trctcm-color-aware|trctcm-color-blind]
no set [cos|ip dscp|phb]
```

Parameters

no <PARAMETERS>

no <PARAMETERS>

Removes this traffic class settings based on the parameters passed

Examples

```
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#show context
class dscp
 set ip dscp 3
 police flow 100000 4000 conform-action transmit violate-action drop
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#no set ip dscp
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#no police flow
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#show context
class dscp
nx9500-6C8809(config-ex3500-qos-policy-map-testPolicyMap-pmap-class-dscp)#
```

description

Configures this EX3500 QoS policy map's description

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 7510

Syntax

```
description <LINE>
```

Parameters

description <LINE>

description <LINE>

Configures this EX3500 QoS policy map's description

- <LINE> - Enter a description that allows to you differentiate it from other policies with similar configuration (should not exceed 64 characters)

Examples

```
nx9500-6C8809(config-ex3500-qos-policy-map-test)#description "This is a test EX3500 QoS
Policy Map"
nx9500-6C8809(config-ex3500-qos-policy-map-test)#show context
ex3500-qos-policy-map test
 description "This is a test EX3500 QoS Policy Map"
 class test
nx9500-6C8809(config-ex3500-qos-policy-map-test)#
```

Related Commands

no

Removes this EX3500 QoS policy map's description

no

Removes this EX3500 QoS policy map's settings. Use this keyword to remove the description and to remove the QoS traffic classification created.

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 7510

Syntax

```
no [class <EX3500-QoS-POLICY-MAP-NAME>|description]
```

Parameters

```
no <PARAMETERS>
```

|                 |                                                                              |
|-----------------|------------------------------------------------------------------------------|
| no <PARAMETERS> | Removes this EX3500 QoS policy map's settings based on the parameters passed |
|-----------------|------------------------------------------------------------------------------|

Examples

The following example shows the EX3500 QoS policy map 'test' settings before the 'no' command are executed:

```
nx9500-6C8809(config-ex3500-qos-policy-map-test)#show context
ex3500-qos-policy-map test
 description "This is a test EX3500 QoS Policy Map"
 class test
nx9500-6C8809(config-ex3500-qos-policy-map-test)#
nx9500-6C8809(config-ex3500-qos-policy-map-test)#no description
nx9500-6C8809(config-ex3500-qos-policy-map-test)#no class test
```

The following example shows the EX3500 QoS policy map 'test' settings after the 'no' command are executed:

```
nx9500-6C8809(config-ex3500-qos-policy-map-test)#show context
ex3500-qos-policy-map test
nx9500-6C8809(config-ex3500-qos-policy-map-test)#
```

### ex3524

Adds a EX3524 switch to the network

The EX3500 series switch is a Gigabit Ethernet layer 2 switch with either 24 or 48 10/100/1000-BASE-T ports, and four SFP transceiver slots for fiber connectivity.

To enable layer 3 adoption of the logged EX3524 switch to a NOC controller, navigate to the EX3524 switch's device configuration mode and execute the following command: controller > host > <IP/HOSTNAME>.

EX3500 devices (EX3524 and EX3548) are layer 2 Gigabit Ethernet switches with either 24 or 48 10/100/1000-BASE-T ports, and four SFP transceiver slots for fiber connectivity. Each 10/100/1000 Mbps port supports both the IEEE 802.3af and IEEE 802.3at-2009 PoE standards. An EX3500 switch has an SNMP-based management agent that provides both in-band and out-of-band management access. The EX3500 switch utilizes an embedded HTTP Web agent and CLI, which in spite of being different from that of the WiNG operating system provides WiNG controllers PoE and port management resources.

The NX 95XX and NX 7510 WiNG managed series service platforms and WiNG VMs can discover, adopt, and partially manage EX3500 series Ethernet switches without modifying the proprietary operating

system running the EX3500 switches. The WiNG service platforms utilize standardized WiNG interfaces to push configuration files to the EX3500 switches, and maintain a translation layer, understood by the EX3500 switch, for statistics retrieval.

**Supported in the following platforms:**

- Service Platforms – NX 95XX, NX 7510

**Syntax**

```
ex3524 <DEVICE-EX3524-MAC>
```

**Parameters**

```
ex3524 <DEVICE-EX3524-MAC>
```

|                     |                                              |
|---------------------|----------------------------------------------|
| <DEVICE-EX3524-MAC> | Specifies the MAC address of a EX3524 switch |
|---------------------|----------------------------------------------|

**Examples**

```
nx9500-6C8809(config)#ex3524 A1-C4-33-6D-66-07
nx9500-6C8809(config-device-A1-C4-33-6D-66-07)#?
EX35xx Device Mode commands:
 hostname Set system's network name
 interface Select an interface to configure
 ip Internet Protocol (IP)
 no Negate a command or set its defaults
 power EX3500 Power over Ethernet Command
 remove-override Remove configuration item override from the device (so
 profile value takes effect)
 upgrade Configures upgrade option for ex3500 system
 use Set setting to use

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-device-A1-C4-33-6D-66-07)#
```

**Related Commands**

|    |                                          |
|----|------------------------------------------|
| no | Removes a EX3524 switch from the network |
|----|------------------------------------------|

**ex3548**

Adds a EX3548 switch to the network

The EX3500 series switch is a Gigabit Ethernet layer 2 switch with either 24 or 48 10/100/1000-BASE-T ports, and four SFP transceiver slots for fiber connectivity.

**Supported in the following platforms:**

- Service Platforms – NX 95XX, NX 7510



## Syntax

```
ex3548 <DEVICE-EX3548-MAC>
```

## Parameters

```
ex3548 <DEVICE-EX3548-MAC>
```

|                     |                                              |
|---------------------|----------------------------------------------|
| <DEVICE-EX3548-MAC> | Specifies the MAC address of a EX3548 switch |
|---------------------|----------------------------------------------|

## Examples

```
nx9500-6C8809(config)#ex3548 22-65-78-09-12-35
nx9500-6C8809(config-device-22-65-78-09-12-35)#?
EX35xx Device Mode commands:
 hostname Set system's network name
 interface Select an interface to configure
 ip Internet Protocol (IP)
 no Negate a command or set its defaults
 power EX3500 Power over Ethernet Command
 remove-override Remove configuration item override from the device (so
 profile value takes effect)
 upgrade Configures upgrade option for ex3500 system
 use Set setting to use

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-device-22-65-78-09-12-35)#
```

## Related Commands

|    |                                          |
|----|------------------------------------------|
| no | Removes a EX3548 switch from the network |
|----|------------------------------------------|

### *firewall-policy*

Configures a firewall policy. This policy defines a set of rules for managing network traffic and prevents unauthorized access to the network behind the firewall.

#### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
firewall-policy <FIREWALL-POLICY-NAME>
```

## Parameters

```
firewall-policy <FIREWALL-POLICY-NAME>
```

|                        |                                                                                                                 |
|------------------------|-----------------------------------------------------------------------------------------------------------------|
| <FIREWALL-POLICY-NAME> | Specify the firewall policy name. If a firewall policy, with the specified name, does not exist, it is created. |
|------------------------|-----------------------------------------------------------------------------------------------------------------|

### Examples

```

nx9500-6C8809(config)#firewall-policy test
nx9500-6C8809(config-fw-policy-test)#?
Firewall policy Mode commands:
 acl-logging Log on flow creating traffic
 alg Enable ALG
 clamp Clamp value
 dhcp-offer-convert Enable conversion of broadcast dhcp offers to
 unicast
 dns-snoop DNS Snooping
 firewall Wireless firewall
 flow Firewall flow
 ip Internet Protocol (IP)
 ip-mac Action based on ip-mac table
 ipv6 Internet Protocol version 6 (IPv6)
 ipv6-mac Action based on ipv6-mac table
 logging Firewall enhanced logging
 no Negate a command or set its defaults
 proxy-arp Enable generation of ARP responses on behalf
 of another device
 proxy-nd Enable generation of ND responses (for IPv6)
 on behalf of another device
 stateful-packet-inspection-l2 Enable stateful packet inspection in layer2
 firewall
 storm-control Storm-control
 virtual-defragmentation Enable virtual defragmentation for IPv4
 packets (recommended for proper functioning
 of firewall)

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or
 terminal

```

```
nx9500-6C8809(config-fw-policy-test)#
```

### Related Commands

|           |                                     |
|-----------|-------------------------------------|
| <b>no</b> | Removes an existing firewall policy |
|-----------|-------------------------------------|



#### Note

For more information on Firewall policy, see [FIREWALL-POLICY](#) on page 1483

### *global-association-list*

Configures a global list of client MAC addresses. Based on the deny or permit rules specified, clients are either allowed or denied access to the managed network.



The global association list serves the same purpose as an Association ACL (Access Control List). However, the Association ACL allows a limited number of entries, a few thousand only, and does not suffice the requirements of a large deployment. This gap is filled by a global association list, which is much larger (with tens of thousands of entries). Both lists co-exist in the system. When an access request comes in, the association ACL is looked up first and if the requesting MAC address is listed in one of the deny ACLs, the association is denied. But, if the requesting client is permitted access, or if in case none of the ACLs list the client's MAC address, the global association ACL is checked. Once authenticated, the client's credentials are cached on the Access Point, and subsequent requests are not referenced to the controller. An entry in an APs credential cache means a pass in the global association list.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
global-association-list <GLOBAL-ASSOC-LIST-NAME>
```

### Parameters

```
global-association-list <GLOBAL-ASSOC-LIST-NAME>
```

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <GLOBAL-ASSOC-LIST-NAME> | Specify the global association list name. If a list with the same name does not exist, it is created. Map this global association list to a device (controller) or a controller profile. Once associated, the controller applies this association list to requests received from all adopted APs. For more information, see <a href="#">use</a> on page 1232. The global association list can also be mapped to a WLAN. The usage of global access lists is controlled on a per-WLAN basis. For more information, see <a href="#">association-list</a> . |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
rfs4000-229D58(config)#global-association-list my-clients
rfs4000-229D58(config-global-assoc-list-my-clients)#
Global Association List Mode commands:
 default-action Configure the default action when the client MAC does not
 match any rule
 deny Specify MAC addresses to be denied
 no Negate a command or set its defaults
 permit Specify MAC addresses to be permitted

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

rfs4000-229D58(config-global-assoc-list-my-clients)#
```

To enable global-association-list controlled client association, execute the following commands:

- 1 Create a global association list, and configure it as shown in the following examples:
 

```
rfs4000-880DA7(config)#global-association-list vtt-list
rfs4000-880DA7(config-global-assoc-list-vtt-list)#permit 01-22-33-44-55-66 description
sample
rfs4000-880DA7(config-global-assoc-list-vtt-list)#permit 40-B8-9A-39-F1-27 description
acer
rfs4000-880DA7(config-global-assoc-list-vtt-list)#permit 42-B8-9A-39-F1-27 description
ami
rfs4000-880DA7(config-global-assoc-list-vtt-list)#permit 6C-40-08-B2-80-6C description
mac
rfs4000-880DA7(config-global-assoc-list-vtt-list)#permit E0-98-61-34-11-47 description
my_mobile
rfs4000-880DA7(config-global-assoc-list-vtt-list)#show context
global-association-list vtt-list
default-action deny
permit 01-22-33-44-55-66 description sample
permit 40-B8-9A-39-F1-27 description acer
permit 42-B8-9A-39-F1-27 description ami
permit 6C-40-08-B2-80-6C description mac
permit E0-98-61-34-11-47 description my_mobile
rfs4000-880DA7(config-global-assoc-list-vtt-list)#
```
- 2 Attach this global association list to the profile or device context of the access point or controller, as shown in the following examples:

On the access point's profile context:



#### Note

Ensure that the global association list is associated with the profile being applied on the access point.

```
rfs4000-880DA7(config-profile-testAP6522)#use global-association-list server
vtt-list
rfs4000-880DA7(config-profile-testAP6522)#show context include-factory | include g
lobal-association-list
service global-association-list blacklist-interval 60
use global-association-list server vtt-list
rfs4000-880DA7(config-profile-testAP6522)#
```

On the access point's device context:

```
ap6522(config-device-B4-C7-99-EA-DF-2C)#use global-association-list server vtt-list
ap6522(config-device-B4-C7-99-EA-DF-2C)#show context include-factory | in
clude global-association-list
use global-association-list server vtt-list
ap6522(config-device-B4-C7-99-EA-DF-2C)#
```

On the controller's device context:

```
rfs4000-880DA7(config-device-00-23-68-88-0D-A7)#use global-association-list server vtt-
list
rfs4000-880DA7(config-device-00-23-68-88-0D-A7)#show context include-factory | in
clude global-association-list
use global-association-list server vtt-list
ap6522(config-device-B4-C7-99-EA-DF-2C)#
```

- 3 Attach this global association list with the WLAN, as shown in the following example:

```
rfs4000-880DA7(config-wlan-GLAssList)#association-list global vtt-list
rfs4000-880DA7(config-wlan-GLAssList)#show context include-factory | include
association-list
association-list global vtt-list
rfs4000-880DA7(config-wlan-GLAssList)#
```

## guest-management-policy

Configures a guest management policy that redirects guest users to a registration portal upon association to a captive portal. Guest users are redirected to an internally (or) externally hosted registration page (registration.html) where previously, not-registered guest users can register. The internally hosted captive portal registration page can be customized based on business requirements.

Use the guest management policy commands to configure parameters, such as E-mail host and SMS gateway along with the credentials required for sending pass code to guest via e-mail and SMS. You can configure up to 32 different guest management policies. Each guest management policy allows you to configure the SMS gateway, SMS message body, E-mail SMTP server, E-mail subject contents, and E-mail message body. Although, at any point-in-time, multiple guest management policies may exist, only one guest management policy can be active per device.

Guest registration is supported only on the NX 95XX and NX 7510 series service platforms. However, the number of user identity entries supported on each varies. It is 2 million and 1 million user-identity entries for the NX 95XX and NX 7510 model service platforms respectively.

### Supported in the following platforms:

- Service Platforms – NX 7510, NX 95XX

### Syntax

```
guest-management <POLICY-NAME>
```

### Parameters

```
guest-management <POLICY-NAME>
```

|               |                                                                                        |
|---------------|----------------------------------------------------------------------------------------|
| <POLICY-NAME> | Specify the guest management policy name. If the policy does not exist, it is created. |
|---------------|----------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config)#guest-management guest
nx9500-6C8809(config-guest-management-guest)#?
Guest Management Mode commands:
 email Email guest-notification configuration
 guest-database-backup Configure guest-database-backup parameters
 guest-database-export Configure guest-database-export parameters
 no Negate a command or set its defaults
 sms SMS guest-notification configuration
 sms-over-smtp Sms-over-smtp configuration to email sms gateway
 address

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-guest-management-guest)#
```

## Related Commands

|                 |                                             |
|-----------------|---------------------------------------------|
| <code>no</code> | Removes an existing guest management policy |
|-----------------|---------------------------------------------|

### guest-management-policy config commands

The following table summarizes guest management policy configuration mode commands:

**Table 22: Guest Management Policy Config Commands**

| Command                                        | Description                                                                                                                                                                                                                                             |
|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>email</code> on page 432                 | Configures guest user e-mail notification settings                                                                                                                                                                                                      |
| <code>guest-database-backup</code> on page 434 | Enables periodic backup of the captive portal's guest registration user database                                                                                                                                                                        |
| <code>guest-database-export</code> on page 435 | Schedules an export of the Guest Management User database to a specified external server                                                                                                                                                                |
| <code>sms</code> on page 436                   | Configures guest user SMS notification settings                                                                                                                                                                                                         |
| <code>sms-over-smtp</code> on page 437         | Configures an e-mail host server along with sender credentials and the recipient's gateway e-mail address to which the message is e-mailed. The gateway server converts the e-mail into SMS and forwards the message to the guest user's mobile device. |
| <code>no</code> on page 439                    | Removes this guest management policy settings                                                                                                                                                                                                           |

#### email

Configures guest user e-mail notification settings. When configured, guest users can register themselves with their e-mail credentials as a primary key for authentication. The captive portal system provides the pass code for their registration. Guest users need to use their registered e-mail, mobile, or member ID and the received pass code for subsequent logins to the captive portal.

Supported in the following platforms:

- Service Platforms — NX 7510, NX 95XX

#### Syntax

```
email [host|message|subject]
email host [<IP/HOSTNAME>|<HOST-ALIAS-NAME>] sender <EMAIL-ADDRESS>
security [none|ssl|starttls] username <USER-NAME> password <PASSWORD>
email message <LINE>
email subject <LINE>
```

#### Parameters

```
email host [<IP/HOSTNAME>|<HOST-ALIAS-NAME>] sender <EMAIL-ADDRESS> security
[none|ssl|starttls] username <USER-NAME> password <PASSWORD>
```

|                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| email                                           | Configures guest user e-mail notification settings                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| host [<IP/<br>HOSTNAME>  <HOST-<br>ALIAS-NAME>] | Configures the SMTP server's IP address or hostname used for guest management e-mail traffic, guest user credential validation, and pass code reception. Optionally you can use an existing host alias to identify the SMTP server host. <ul style="list-style-type: none"> <li>• &lt;IP/HOSTNAME&gt; - Specify the SMTP server's IPv4 address or hostname.</li> <li>• &lt;HOST-ALIAS-NAME&gt; - Specify the host alias name (should be existing and configured). Consider providing the host as an alias. A host alias is a configuration item that maps the alias to a hostname. Once created, it can be used across different configuration modes. Where ever used the alias is replaced by the associated hostname.</li> </ul> |
| sender <EMAIL-<br>ADDRESS>                      | Configures the sender's name for the guest user receiving the passcode required for registering their guest E-mail credentials using SMTP. <ul style="list-style-type: none"> <li>• &lt;EMAIL-SENDER&gt; - Specify the sender's name (should not exceed 100 characters).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| security [none ssl <br>starttls]                | Configures the encryption protocol used by the SMTP server when communicating the pass code <ul style="list-style-type: none"> <li>• none - No encryption used. Use if no additional user authentication is needed beyond the required username and password combination.</li> <li>• SSL - Uses SSL encryption. This is the default setting.</li> <li>• STARTTLS - Uses STARTTLS encryption</li> </ul>                                                                                                                                                                                                                                                                                                                             |
| username <USER-<br>NAME>                        | Configures a username unique to this SMS guest management configuration. After configuring the username, specify the associated password. Ensure that the password is correctly provided to receive the pass code required for registering guest user credentials with SMS. <ul style="list-style-type: none"> <li>• &lt;USER-NAME&gt; - Specify the username (should not exceed 100 characters).</li> </ul>                                                                                                                                                                                                                                                                                                                       |
| password<br><PASSWORD>                          | Configures the password associated with the specified SMTP user name <ul style="list-style-type: none"> <li>• &lt;PASSWORD&gt; - Specify the password (should not exceed 63 characters).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

email message <LINE>

|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| email          | Configures guest user e-mail notification content                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| message <LINE> | Configures the content of the e-mail sent to the guest user notifying the pass code (should not exceed 1024 characters) <ul style="list-style-type: none"> <li>• &lt;LINE&gt; - Specify the message content. When entering the message, use the following tags: <p>GM-NAME - for the guest user's name</p> <p>GM_PASSCODE - for the pass code</p> <p>CR-NL - to enter a new line</p> <p>For example: Dear GM_NAME, CR-NL your internet access pass code is GM_PASSCODE. CR-NL Use this for internet access.</p> </li> </ul> |

email subject <LINE>

|                |                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| email          | Configures guest user e-mail notification subject line                                                                                                                                                                                                                                                                                                                                        |
| subject <LINE> | Configures the subject line of the e-mail sent to the guest user notifying the pass code (should not exceed 100 characters) <ul style="list-style-type: none"> <li>• &lt;LINE&gt; - Specify the subject line content. When entering the subject line, use the following tag:<br/><br/>GM-NAME - for the guest user's name<br/><br/>For example: GM_NAME, your internet access code</li> </ul> |

### Examples

```

nx9500-6C8809(config-guest-management-test)#email host 192.168.13.10 sender
bob@extremenetworks.com security ssl username guest1 password guest1@123
nx9500-6C8809(config-guest-management-test)#show context
guest-management test
 email host 192.168.13.10 sender bob@extremenetworks.com security ssl username guest1
 password guest1@123
nx9500-6C8809(config-guest-management-test)#
nx9500-6C8809(config-guest-management-test2)#email message Dear GM_Guest2, CR-NL
Your internet access passcode is GM_Guest2. CR-NL Use this for internet access.
nx9500-6C8809(config-guest-management-test2)#email subject GM_Guest2 Your internet access
code
nx9500-6C8809(config-guest-management-test2)#show context
guest-management test2
 email subject GM_Guest2 Your internet access code
 email message Dear GM_Guest2, CR-NL Your internet access passcode is GM_Guest2. CR-NL
 Use this for internet access.
nx9500-6C8809(config-guest-management-test2)#

```

### Related Commands

|    |                                                                               |
|----|-------------------------------------------------------------------------------|
| no | Removes the e-mail settings used to send notification mails to the guest user |
|----|-------------------------------------------------------------------------------|

## guest-database-backup

Enables periodic backup of a captive portal's guest registration user database. This option is enabled by default.

Supported in the following platforms:

- Service Platforms — NX 7510, NX 95XX

### Syntax

```
guest-database-backup enable {<TIME>}
```

### Parameters

```
guest-database-backup enable {<TIME>}
```

|                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| guest-database-backup enable {<TIME>} | Enables periodic backup of a captive portal's guest registration user database. This command also allows you to configure the time at which the system starts backing up the database. The default backup-start time is '00:00' (midnight every day). <ul style="list-style-type: none"> <li>• &lt;TIME&gt; - Optional. Resets the periodic database backup-start time to a user-defined value in the HH;MM format. When specified, the system starts periodic backup of the database, every day, at the specified time.</li> </ul> |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-guest-management-test)#guest-database-backup enable 12:30
nx9500-6C8809(config-guest-management-test)#show context
guest-management test
 guest-database-backup enable 12:30
nx9500-6C8809(config-guest-management-test)#
```

## Related Commands

|                 |                                                                                 |
|-----------------|---------------------------------------------------------------------------------|
| <code>no</code> | Disables periodic backup of a captive portal's guest registration user database |
|-----------------|---------------------------------------------------------------------------------|

## guest-database-export

Schedules an export of the Guest Management user database to a specified external server. This option is enabled by default.

Supported in the following platforms:

- Service Platforms — NX 7510, NX 95XX

## Syntax

```
guest-database-export <TIME> frequency <1-168> url-directory <URL>
{(format [csv/json]/last-visit-within <1-168>)}
```

## Parameters

```
guest-database-export <TIME> frequency <1-168> url-directory <URL>
{(format [csv/json]/last-visit-within <1-168>)}
```

|                              |                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| guest-database-export <TIME> | Schedules an export of the Guest Management User collection to an external server <ul style="list-style-type: none"><li>• &lt;TIME&gt; - Configures the start time of the export operation in the HH:MM format</li></ul>                                                                                                                                          |
| frequency <1-168>            | Configures the user collection export frequency in hours <ul style="list-style-type: none"><li>• &lt;1-168&gt; - Configures the frequency from 1 - 168 hours. If the frequency is set at 3 hours, the user database is exported once in every 3 hours. The default is 4 hours.</li></ul>                                                                          |
| url-directory <URL>          | Configures external server's URL and directory to where the collection is exported <ul style="list-style-type: none"><li>• &lt;URL&gt; - Specify the external server's URL</li></ul>                                                                                                                                                                              |
| format [csv/json]            | Optional. Configures the file format <ul style="list-style-type: none"><li>• csv - Exports collection to the specified location in CSV format. This is the default setting.</li><li>• json - Exports collection to the specified location in JSON format</li></ul>                                                                                                |
| last-visit-within <1-168>    | Configures a filters guest users who have last visited within a specified period of time <ul style="list-style-type: none"><li>• &lt;1-168&gt; - Specify a time period from 1 - 168 hours. If for example, the last-visit-within value is set at 2 hours, then only the last two hours guest user collections will be exported. The default is 4 hours.</li></ul> |

## Examples

```
nx9500-6C8809(config-guest-management-gml)#guest-database-export 10:30 frequency 6 url-
directory ftp://admin:xxxxxx@192.168.13.10/dbe_dir format json last-visit-within 168
nx9500-6C8809(config-guest-management-test)#show context
guest-management test
 guest-database-export 12:30 frequency 20 url-directory ftp://admin:xxxxxx@192.168.13.10/
 dbe_dir format json last-visit-within 168
nx9500-6C8809(config-guest-management-test)#
```

## Related Commands

no

Reverts the guest database export parameters to default

sms

Configures guest user SMS notification settings

When configured, guest users can register themselves with their e-mail or mobile device ID as the primary key for authentication. The captive portal provides the pass code for registration. Guest users use their registered e-mail or mobile device ID and the received pass code for subsequent logins to the captive portal.



#### Note

When using SMS, ensure that the WLAN's mode of authentication is set to none and the mode of registration is set to user. In other words, captive portal authentication must always enforce guest registration.

SMS is similar to MAC address-based self registration, but in addition the captive portal sends an SMS message, containing an access code, to the user's mobile phone number provided at the time of registration. The captive portal verifies the code, returns the Welcome page and provides access. This allows the administrator to verify the phone number provided and can be traced back to a specific individual should the need arise.

The default gateway used with SMS is Clickatell. A pass code can be sent with SMS to the guest user directly using Clickatell, or the pass code can be sent via e-mail to the SMS Clickatell gateway server, and Clickatell sends the pass code SMS to the guest user.

Supported in the following platforms:

- Service Platforms — NX 7510, NX 95XX

#### Syntax

```
sms [host|message] sms host clickatell username <USER-NAME> password <PASSWORD>
api-id <ID> user-agent <PYCLICKATELL> {source-number <WORD>}
sms message <LINE>
```

#### Parameters

```
sms host clickatell username <USER-NAME> password <PASSWORD>
api-id <ID> user-agent <PYCLICKATELL> {source-number <WORD>}
```

|                      |                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| sms                  | Configures guest user SMS notification settings                                                                                                                                                                                                                                                                                                                                                           |
| host clickatell      | By default, clickatell is the host SMS gateway server resource. Upon receiving the pass code e-mail, the SMS gateway sends the actual notification pass code SMS to the guest user.                                                                                                                                                                                                                       |
| username <USER-NAME> | Configures a username unique to this SMS guest management configuration. After configuring the username, specify the associated password. Ensure that the password is correctly provided to receive the pass code required for registering guest user credentials with SMS. <ul style="list-style-type: none"><li>• &lt;USER-NAME&gt; - Specify the username (should not exceed 32 characters).</li></ul> |
| password <PASSWORD>  | Configures the password associated with the specified username <ul style="list-style-type: none"><li>• &lt;PASSWORD&gt; - Specify the password (should not exceed 63 characters).</li></ul>                                                                                                                                                                                                               |
| api-id <ID>          | Set a 32 character maximum API ID <ul style="list-style-type: none"><li>• &lt;API-ID&gt; - Specify the API ID (should not exceed 32 characters).</li></ul>                                                                                                                                                                                                                                                |



|                           |                                                                                                                                                                                                                                                                |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| user-agent <PYCLICKATELL> | Since the SMS service provider by default is Clickatell, set the user agent name to pyclickatell. The user-agent value ensures the Clickatell SMS gateway server and its related credentials, needed for sending the pass code to guest users, are configured. |
| source-number <WORD>      | Optional. Configures the long-address or the from-number associated with this Clickatell user account <ul style="list-style-type: none"> <li>&lt;WORD&gt; – Specify the source number (should not exceed 32 characters).</li> </ul>                            |

sms message <LINE>

|                |                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| sms            | Configures guest user SMS notification content                                                                                                                                                                                                                                                                                                                                                                                            |
| message <LINE> | Configures the content of the SMS sent to the guest user notifying the pass code (should not exceed 1024 characters) <ul style="list-style-type: none"> <li>&lt;LINE&gt; – Specify the message content. When entering the message, use the following tags: <p>GM-NAME – for the guest user’s name</p> <p>GM_PASSCODE – for the pass code</p> <p>For example: Dear GM_NAME, your internet access pass code is GM_PASSCODE.</p> </li> </ul> |

### Examples

```

nx9500-6C8809(config-guest-management-test)#sms host clickatell username guest1
password guest1@123 api-id test user-agent pyclickatell
nx9500-6C8809(config-guest-management-test)#sms message Dear guest1, Your passcode for
internet access is GM-guest1
nx9500-6C8809(config-guest-management-test)#show context
guest-management test
 email host 192.168.13.10 sender bob@extremenetworks.com security ssl username guest1
password guest1@123
 sms host clickatell username guest1 password guest1@123 api-id test user-agent
pyclickatell
 sms message Dear guest1, Your passcode for internet access is GM-guest1
nx9500-6C8809(config-guest-management-test)#

```

### Related Commands

|    |                                                             |
|----|-------------------------------------------------------------|
| no | Removes the SMS settings used to send SMS to the guest user |
|----|-------------------------------------------------------------|

### sms-over-smtp

Configures an e-mail host server (for example: smtp.gmail.com) along with sender related credentials and the recipient gateway e-mail address to which the message is E-mailed. The gateway server converts the e-mail into SMS and sends the message to the guest user’s mobile device.

When sending an e-mail, the e-mail client interacts with a SMTP server to handle the content transmission. The SMTP server on the host may have conversations with other SMTP servers to deliver the e-mail.

Supported in the following platforms:

- Service Platforms — NX 7510, NX 95XX

## Syntax

```
sms-over-smtp [host | message | subject]
sms-over-smtp host [<IP/HOSTNAME> | <HOST-ALIAS-NAME>] sender <EMAIL-ADDRESS>
security [none | ssl | starttls] username <USER-NAME> password <PASSWORD> recipient <EMAIL-ADDRESS>
sms-over-smtp message <LINE>
sms-over-smtp subject <LINE>
```

## Parameters

```
sms-over-smtp host [<IP/HOSTNAME> | <HOST-ALIAS-NAME>] sender <EMAIL-ADDRESS> security
[none | ssl | starttls] username <USER-NAME> password <PASSWORD> recipient <EMAIL-ADDRESS>
```

|                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| sms-over-smtp                              | Configures guest user SMS over SMTP notification settings                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| host [ <IP/HOSTNAME>   <HOST-ALIAS-NAME> ] | Configures the SMS gateway server resource's IPv4 address or hostname used for guest management SMS over SMTP traffic, guest user credential validation and pass code reception. Optionally you can use an existing host alias to identify the SMS gateway server resource. <ul style="list-style-type: none"><li>• &lt;IP/HOSTNAME&gt; - Specify the SMTP gateway server resource's IP address or hostname.</li><li>• &lt;HOST-ALIAS-NAME&gt; - Specify the host alias name (should existing and configured). Consider providing the host as an alias. A host alias is a configuration item that maps the alias to a hostname. Once created, it can be used across different configuration modes. Where ever used the alias is replaced by the associated hostname.</li></ul> |
| sender <EMAIL-ADDRESS>                     | Configures the sender's e-mail address. The sender here is the guest user receiving the pass code. Guest users require this pass code for registering their guest e-mail credentials using SMTP. <ul style="list-style-type: none"><li>• &lt;EMAIL-ADDRESS&gt; - Specify the e-mail address (should not exceed 64 characters).</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| security [none   ssl   starttls]           | Configures the encryption protocol used by the SMTP server when communicating the pass code <ul style="list-style-type: none"><li>• none - No encryption used. Use if no additional user authentication is needed beyond the required username and password combination.</li><li>• SSL - Uses SSL encryption. This is the default setting.<ul style="list-style-type: none"><li>• STARTTLS - Uses STARTTLS encryption</li></ul></li></ul>                                                                                                                                                                                                                                                                                                                                      |
| username <USER-NAME>                       | Configures a username unique to this SMTP guest management configuration. After configuring the username, specify the associated password. Ensure that the correct password is provided to receive the pass code required for registering guest user credentials with SMTP. <ul style="list-style-type: none"><li>• &lt;USER-NAME&gt; - Specify the username (should not exceed 64 characters).</li></ul>                                                                                                                                                                                                                                                                                                                                                                      |
| password <PASSWORD>                        | Configures the password associated with the specified SMTP user name <ul style="list-style-type: none"><li>• &lt;PASSWORD&gt; - Specify the password (should not exceed 64 characters).</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| recipient <EMAIL-ADDRESS>                  | Configures the e-mail recipient's e-mail address <ul style="list-style-type: none"><li>• &lt;EMAIL-ADDRESS&gt; - Specify the recipient's e-mail address (should not exceed 64 characters in length).</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

```
sms-over-smtp message <LINE>
```

|                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>sms-over-smtp message &lt;LINE&gt;</pre> | <p>Configures guest user SMS over SMTP notification message content</p> <p>Configures the content of the SMS over SMTP sent to the guest user notifying the pass code (should not exceed 1024 characters)</p> <ul style="list-style-type: none"> <li>• &lt;LINE&gt; - Specify the message content. When entering the message, use the following tags: <ul style="list-style-type: none"> <li>GM-NAME - for the guest user's name</li> <li>GM_PASSCODE - for the pass code</li> <li>CR-NL - to enter a new line</li> </ul> </li> </ul> <p>For example: Dear GM_NAME, CR-NL your internet access pass code is GM_PASSCODE. CR-NL Use this access code for internet access.</p> |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
sms-over-smtp subject <LINE>
```

|                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>sms-over-smtp subject &lt;LINE&gt;</pre> | <p>Configures guest user e-mail notification subject line content</p> <p>Configures the subject line of the SMS over SMTP sent to the guest user notifying the pass code (should not exceed 100 characters)</p> <ul style="list-style-type: none"> <li>• &lt;LINE&gt; - Specify the subject line content. When entering the subject line, use the following tag: <ul style="list-style-type: none"> <li>GM-NAME - for the guest user's name</li> </ul> </li> </ul> <p>For example: GM_NAME, your internet access code</p> |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config-guest-management-test3)#sms-over-smtp host test sender
bob@extremenetworks.com security ssl username bob password bob@123 recipient
john@extremenetworks.com
nx9500-6C8809(config-guest-management-test3)#show context
guest-management test3
 sms-over-smtp host test sender bob@extremenetworks.com security ssl username bob password
bob@123 recipient john@extremenetworks.com
nx9500-6C8809(config-guest-management-test3)#
```

### Related Commands

|           |                                                                       |
|-----------|-----------------------------------------------------------------------|
| <b>no</b> | Removes the SMS over SMTP settings used to send SMS to the guest user |
|-----------|-----------------------------------------------------------------------|

no

Removes this guest management policy settings

Supported in the following platforms:

- Service Platforms — NX 7510, NX 95XX

### Syntax

```
no [email | guest-database-backup | guest-database-export | sms | sms-over-smtp]
no email [host | message | subject]
no guest-database-backup enable
no guest-database-export
no gmd report-generation enable
no sms [host | message]
no sms-over-smtp [host | message | subject]
```

## Parameters

no <PARAMETERS>

|                 |                                                                              |
|-----------------|------------------------------------------------------------------------------|
| no <PARAMETERS> | Removes this guest management policy settings based on the parameters passed |
|-----------------|------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-guest-management-test3)#show context
guest-management test3
 sms-over-smtp host test sender bob@extremenetworks.com security ssl username bob password
bob@123 recipient john@extremenetworks.com
nx9500-6C8809(config-guest-management-test3)#
nx9500-6C8809(config-guest-management-test)#no sms-over-smtp host
nx9500-6C8809(config-guest-management-test3)#show context
guest-management test3
nx9500-6C8809(config-guest-management-test3)#
```

## host

Enters the configuration context of a remote device using its hostname

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

host <DEVICE-NAME>

## Parameters

host <DEVICE-NAME>

|               |                                                                                                                          |
|---------------|--------------------------------------------------------------------------------------------------------------------------|
| <DEVICE-NAME> | Specify the device's hostname. All discovered devices are displayed when 'Tab' is pressed to auto complete this command. |
|---------------|--------------------------------------------------------------------------------------------------------------------------|

## Examples

```
NOC-NX9500(config)#host [TAB]
ap7522-8330A4 ap8163-74B45C
default/ap7522-8330A4 default/ap8163-74B45C
default/NOC-NX9500 default/RFS6K-SITE1-VLAN20
NOC-NX9500 RFS6K-SITE1-VLAN20
RFS6K-SITE2-VLAN192 default/RFS6K-SITE2-VLAN192
NOC-NX9500(config)#host ap7522-8330A4
NOC-NX9500(config-device-84-24-8D-83-30-A4)#
```

## inline-password-encryption

Stores the encryption key in the startup configuration file

By default, the encryption key is not stored in the startup-config file. Use the inline-password-encryption command to move the encrypted key to the startup-config file. This command uses the master key to encrypt the password, then moves it to the startup-config file.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
inline-password-encryption
```

### Parameters

None

### Usage Guidelines

When the configuration file is imported to a different device, it first decrypts the encryption key using the default key and then decrypts the rest of the configuration using the administrator configured encryption key.

### Examples

The following command uses the specified password for encryption key and stores it outside of startup-config:

```
nx9500-6C8809(config)#password-encryption secret 2 12345678
nx9500-6C8809(config)#commit write memory
```

The following command moves the same password to the startup-config and encrypts it with the master key:

```
nx9500-6C8809(config)#inline-password-encryption
```

### Related Commands

|                                              |                                                                          |
|----------------------------------------------|--------------------------------------------------------------------------|
| <code>no</code>                              | Disables storing of the encryption key in the startup configuration file |
| <code>password-encryption</code> on page 487 | Enables password encryption                                              |

### *iot-device-type-imagotag-policy*

Creates an IoT Device-Type ImagoTag policy and enters its configuration mode. Use this option to enable support for SES-imagotag's ESL (Electronic Shelf Label) tags on WiNG APs with USB interfaces.

ESL tags are small, battery-powered devices used by retail businesses to display information, such as product code, pricing, etc. These tags are activated, configured, and managed through an SES-ImagoTag provided server. The tags and server communicate through an ESL communicator (a USB dongle), connected to the USB port on the WiNG AP. This communication is over the 2.4 GHz band using a proprietary RF protocol. The ESL communicator acts as a bridge between the tags and the server, using WiNG AP as an infrastructure device.

This policy, when applied on an AP, enables the AP recognize the ESL communicator, and facilitate communication between communicator and tags.

The policy can be applied to the AP's self (in case of stand alone AP), or pushed to the AP through the adopting controller. In the latter case, apply the policy on the AP's profile.

### Supported in the following platforms:

- Access Points — AP 8432
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000



#### Note

The policy is applicable only on the AP 8432 model access point, which supports the USB interface.

### Syntax

```
iot-device-type-imagotag-policy <POLICY-NAME>
```

### Parameters

```
iot-device-type-imagotag-policy <POLICY-NAME>
```

|                                               |                                                                                                                                 |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| iot-device-type-imagotag-policy <POLICY-NAME> | Specify an IoT Device Type ImagoTag policy name. If another policy by the specified name does not exist, the policy is created. |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|

### Example

```
nx9500-6C8809(config)#iot-device-type-imagotag-policy ImagoTagPolicy
nx9500-6C8809(config-iot-device-type-imagotag-policy-ImagoTagPolicy)#?
Iot ImagoTag Policy Mode commands:
 channel Auto channel selection
 enable Enable ESL communicator
 fcc-mode Enable fcc compatibility mode on ESL communicator
 no Negate a command or set its defaults
 output-power Maximum output power
 payload-size Configure payload size
 ssl Enable ssl on ESL communicator
 window-size Configure window size

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-iot-device-type-imagotag-policy-ImagoTagPolicy)#
```

### Related Commands

|                                                  |                                                       |
|--------------------------------------------------|-------------------------------------------------------|
| <code>no (global-config-mode) on</code> page 475 | Removes the specified IoT Device Type ImagoTag policy |
|--------------------------------------------------|-------------------------------------------------------|

### iot-device-type-imagotag-policy config commands

The following table summarizes IoT Device-Type ImagoTag policy configuration mode commands:

**Table 23: IoT-Device-Type Imagotag Policy**

| Command                                  | Description                                                                                                    |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| <a href="#">channel</a> on page 443      | Configures the channel assigned for ESL communicator to tag communication in the 2.4 GHz band                  |
| <a href="#">enable</a> on page 443       | Enables the ESL communicator                                                                                   |
| <a href="#">fcc-mode</a> on page 444     | Enables the FCC compatibility mode on the ESL communicator                                                     |
| <a href="#">output-power</a> on page 444 | Configures the maximum output power for the ESL communicator                                                   |
| <a href="#">payload-size</a> on page 445 | Configures the maximum payload size in packets exchanged between ESL communicator and tags                     |
| <a href="#">ssl</a> on page 447          | Enables SSL (Secure Socket Layer) encryption mode of communication between the AP and the SES-imagotag server. |
| <a href="#">window-size</a> on page 446  | Configures the transmission window size for messages exchanged between ESL communicator and tags.              |
| <a href="#">no</a> on page 447           | Reverts this IoT Device-Type Imagotag policy settings to default values                                        |

## channel

Manually configures the channel assigned for ESL communicator to tag communication in the 2.4 GHz band. Or, enables ACS (Auto-Channel Selection) mode.

Supported in the following platforms:

- Access Points — AP 8432
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
channel [<0-10>|acs]
```

### Parameters

```
channel [<0-10>|acs]
```

|                      |                                                                                                                                                                                                                                                                                        |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| channel [<0-10> acs] | <p>Configures the 2.4 GHz frequency channel, using one of the following options:</p> <ul style="list-style-type: none"> <li>• &lt;0-10&gt; – Manually configures the channel from 0 - 10.</li> <li>• acs – Enables ACS channel selection mode. This is the default setting.</li> </ul> |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config-iot-device-type-imagotag-policy-ImagoTagPolicy)#channel 9
nx9500-6C8809(config-iot-device-type-imagotag-policy-ImagoTagPolicy)#show context
iot-device-type-imagotag-policy ImagoTagPolicy
 channel 9
nx9500-6C8809(config-iot-device-type-imagotag-policy-ImagoTagPolicy)#
```

### Related Commands

|                                |                                           |
|--------------------------------|-------------------------------------------|
| <a href="#">no</a> on page 447 | Reverts the channel selection mode to ACS |
|--------------------------------|-------------------------------------------|

## enable

Enables the ESL communicator

Supported in the following platforms:

- Access Points — AP 8432
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

`enable`

Parameters

None

Examples

```
nx9500-6C8809(config-iot-device-type-imagotag-policy-ImagoTagPolicy)#enable
nx9500-6C8809(config-iot-device-type-imagotag-policy-ImagoTagPolicy)#show context
 iot-device-type-imagotag-policy ImagoTagPolicy
 enable
 channel 9
nx9500-6C8809(config-iot-device-type-imagotag-policy-ImagoTagPolicy)#
```

Related Commands

|                             |                               |
|-----------------------------|-------------------------------|
| <code>no</code> on page 447 | Disables the ESL communicator |
|-----------------------------|-------------------------------|

## fcc-mode

Enables the FCC (Federal Communications Commission) compatibility mode on the ESL communicator. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP 8432
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

`fcc-mode`

Parameters

None

Examples

```
nx9500-6C8809(config-iot-device-type-imagotag-policy-ImagoTagPolicy)#fcc-mode
nx9500-6C8809(config-iot-device-type-imagotag-policy-ImagoTagPolicy)#show context
 iot-device-type-imagotag-policy ImagoTagPolicy
 enable
 fcc-mode
 channel 9
nx9500-6C8809(config-iot-device-type-imagotag-policy-ImagoTagPolicy)#
```

Related Commands

|                             |                                 |
|-----------------------------|---------------------------------|
| <code>no</code> on page 447 | Disables FCC compatibility mode |
|-----------------------------|---------------------------------|

## output-power

Configures the maximum output power for the ESL communicator.

Supported in the following platforms:

- Access Points — AP 8432



- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

`output-power [Level-A|Level-B|Level-C|Level-D|Level-E|Level-F|Level-G|Level-H]`

#### Parameters

`output-power [Level-A|Level-B|Level-C|Level-D|Level-E|Level-F|Level-G|Level-H]`

|                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>output-power [Level-A Level-B Level-C Level-D Level-E Level-F Level-G Level-H]</code> | <p>Configure the ESL communicator's output power in dBm. The options are:</p> <ul style="list-style-type: none"> <li>• Level-A - 1 dBm. This is the default setting.</li> <li>• Level-B - -4 dBm</li> <li>• Level-C - -6 dBm</li> <li>• Level-D - -12 dBm</li> <li>• Level-E - 0 dBm</li> <li>• Level-F - -2 dBm</li> <li>• Level-G - -8 dBm</li> <li>• Level-H - -10 dBm</li> </ul> <p><b>Note:</b> SES-Imagotags recommends NOT to change the default setting, which is in conformance to various country/region specific RF regulations.</p> |
|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```

nx9500-6C8809(config-iot-device-type-imagotag-policy-ImagoTagPolicy)#output-power Level-B
nx9500-6C8809(config-iot-device-type-imagotag-policy-ImagoTagPolicy)#show context
 iot-device-type-imagotag-policy ImagoTagPolicy
 enable
 output-power Level-B
 fcc-enable
 channel 9
nx9500-6C8809(config-iot-device-type-imagotag-policy-ImagoTagPolicy)#

```

#### Related Commands

|                             |                                                                  |
|-----------------------------|------------------------------------------------------------------|
| <code>no</code> on page 447 | Reverts the ESL communicator's output-power to default (Level-A) |
|-----------------------------|------------------------------------------------------------------|

### payload-size

Configures the maximum size of the payload in packets exchanged between ESL communicator and tags

Supported in the following platforms:

- Access Points — AP 8432
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

`payload-size <1-32>`

#### Parameters

`payload-size <1-32>`

payload-size <1-32>

Configures the packet's payload size

- <1-32> – Specify the value from 1 - 32 bytes. The default setting is 32 bytes.

**Note:** SES-Imagotags recommends NOT to change the default setting.

#### Examples

```
nx9500-6C8809(config-iot-device-type-imagotag-policy-ImagoTagPolicy)#payload-size 25
nx9500-6C8809(config-iot-device-type-imagotag-policy-ImagoTagPolicy)#show context
 iot-device-type-imagotag-policy ImagoTagPolicy
 enable
 output-power Level-B
 payload-size 25
 fcc-enable
 channel 9
nx9500-6C8809(config-iot-device-type-imagotag-policy-ImagoTagPolicy)#
```

#### Related Commands

**no** on page 447

Reverts the payload size to default (32 bytes)

#### window-size

Configures the transmission window size for messages exchanged between ESL communicator and tags

Supported in the following platforms:

- Access Points — AP 8432
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

window-size <1-14>

#### Parameters

window-size <1-14>

window-size <1-14>

Configures the window size

- <1-14> – Specify a value from 1 - 14 bytes. The default value is 14 bytes.

**Note:** SES-Imagotags recommends NOT to change the default setting.

#### Examples

```
nx9500-6C8809(config-iot-device-type-imagotag-policy-ImagoTagPolicy)#window-size 12
nx9500-6C8809(config-iot-device-type-imagotag-policy-ImagoTagPolicy)#show context
 iot-device-type-imagotag-policy ImagoTagPolicy
 enable
 output-power Level-B
 window-size 12
 payload-size 25
 port 200
 ssl-enable
 fcc-enable
 channel 9
nx9500-6C8809(config-iot-device-type-imagotag-policy-ImagoTagPolicy)#
```

## Related Commands

|                |                                      |
|----------------|--------------------------------------|
| no on page 447 | Reverts the window-size to 14 bytes. |
|----------------|--------------------------------------|

## ssl

Enables secure, encrypted communication over the SSL (Secure Socket Layer) between the AP and SES-imagotag server. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP 8432
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

ssl

## Parameters

None

## Examples

```
nx9500-6C8809(config-iot-device-type-imagotag-policy-ImagoTagPolicy)#ssl
nx9500-6C8809(config-iot-device-type-imagotag-policy-ImagoTagPolicy)#show context
 iot-device-type-imagotag-policy ImagoTagPolicy
 enable
 output-power Level-B
 payload-size 25
 port 200
 ssl
 fcc-enable
 channel 9
nx9500-6C8809(config-iot-device-type-imagotag-policy-ImagoTagPolicy)#
```

## Related Commands

|                |                                               |
|----------------|-----------------------------------------------|
| no on page 447 | Disables SSL encryption mode of communication |
|----------------|-----------------------------------------------|

## no

Reverts this IoT Device-Type Imagotag policy settings to default values

Supported in the following platforms:

- Access Points — AP 8432
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

no [channel|enable|fcc-mode|output-power|payload-size|port|ssl|window-size]

## Parameters

no <PARAMETERS>

|                 |                                                                        |
|-----------------|------------------------------------------------------------------------|
| no <PARAMETERS> | Reverts this IoT Device-Type Imagotag policy settings to default value |
|-----------------|------------------------------------------------------------------------|

## Examples

The following example shows the ImagoTag policy settings before the `no` commands are executed.

```
nx9500-6C8809(config-iot-device-type-imagotag-policy-ImagoTagPolicy)#show context
 iot-device-type-imagotag-policy ImagoTagPolicy
 enable
 output-power Level-B
 window-size 12
 payload-size 25
 ssl-enable
 fcc-enable
 channel 9
nx9500-6C8809(config-iot-device-type-imagotag-policy-ImagoTagPolicy)#
nx9500-6C8809(config-iot-device-type-imagotag-policy-ImagoTagPolicy)#no payload-size
nx9500-6C8809(config-iot-device-type-imagotag-policy-ImagoTagPolicy)#no window-size
```

The following example shows the ImagoTag policy settings after the 'no' commands are executed.

```
nx9500-6C8809(config-iot-device-type-imagotag-policy-ImagoTagPolicy)#show context
 iot-device-type-imagotag-policy ImagoTagPolicy
 enable
 output-power Level-B
 ssl-enable
 fcc-enable
 channel 9
nx9500-6C8809(config-iot-device-type-imagotag-policy-ImagoTagPolicy)#
```

*ip*

Creates an ACL (access control list) and enters its configuration modeS

Access lists define access permissions to the network using a set of rules. Each rule specifies an action taken when a packet matches the rule. If the action is deny, the packet is dropped. If the action is permit, the packet is allowed.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
ip [access-list|ex3500-ext-access-list|ex3500-std-access-list|snmp-access-list]
ip ex3500-ext-access-list <EX3500-EXT-ACL-NAME>
ip ex3500-std-access-list <EX3500-STD-ACL-NAME>
ip access-list <IP-ACL-NAME>
ip snmp-access-list <IP-SNMP-ACL-NAME>
```

#### Parameters

```
ip access-list <IP-ACL-NAME>
```

|                           |                                                                                           |
|---------------------------|-------------------------------------------------------------------------------------------|
| access-list <IP-ACL-NAME> | Creates an IP ACL and enters its configuration mode                                       |
|                           | • <IP-ACL-NAME> - Specify the ACL name. If the access list does not exist, it is created. |

```
ip ex3500-ext-access-list <EX3500-EXT-ACL-NAME>
```

|                                              |                                                                                                                                                                                                                                                  |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ex3500-ext-access-list <EX3500-EXT-ACL-NAME> | <p>Creates an EX3500 Extended ACL and enters its configuration mode</p> <ul style="list-style-type: none"> <li>• &lt;EX3500-EXT-ACL-NAME&gt; - Specify the ACL name. If an ACL with the specified name does not exist, it is created.</li> </ul> |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
ip ex3500-std-access-list <EX3500-STD-ACL-NAME>
```

|                                              |                                                                                                                                                                                                                                                  |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ex3500-std-access-list <EX3500-STD-ACL-NAME> | <p>Creates an EX3500 Standard ACL and enters its configuration mode</p> <ul style="list-style-type: none"> <li>• &lt;EX3500-EXT-ACL-NAME&gt; - Specify the ACL name. If an ACL with the specified name does not exist, it is created.</li> </ul> |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
ip snmp-access-list <IP-SNMP-ACL-NAME>
```

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| snmp-access-list <IP-SNMP-ACL-NAME> | <p>Creates a SNMP IP ACL and enters its configuration mode. An SNMP IP ACL is an access control mechanism that uses a combination of IP ACL and SNMP community string. SNMP performs network management functions using a data structure called a MIB. SNMP is widely implemented but not very secure, since it uses only text community strings for accessing controller or service platform configuration files.</p> <p>Use SNMP ACLs (firewalls) to help reduce SNMP's vulnerabilities, as SNMP traffic can be easily exploited to produce a DoS.</p> <ul style="list-style-type: none"> <li>• &lt;IP-SNMP-ACL-NAME&gt; - Specify the SNMP IP ACL name. If the access list does not exist, it is created. After creating the SNMP ACL, define the deny/permit rules based on the network and/or host IP addresses. Once created and configured, link this SNMP IP ACL with a SNMP community string.</li> </ul> <p>To link the SNMP community string with the SNMP IP ACL, in the management-policy-config-mode, use the following command: <b>snmp-server &gt; community &lt;COMMUNITY-STRING&gt; &gt; [ro rw] &gt; ip-snmp-access-list &lt;IP-SNMP-ACL-NAME&gt;</b>.</p> |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```

nx9500-6C8809(config)#ip access-list test
nx9500-6C8809(config-ip-acl-test)#?
ACL Configuration commands:
 deny Specify packets to reject
 disable Disable rule if not needed
 no Negate a command or set its defaults
 permit Specify packets to forward

 clrscr Clears the display screen
 commit Commit all changes made in this session
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-ip-acl-test)#
nx9500-6C8809(config)#ip snmp-access-list SNMPACL
nx9500-6C8809(config-ip-snmp-acl-SNMPACL)#?
SNMP ACL Configuration commands:
 deny Specify packets to reject
 no Negate a command or set its defaults
 permit Specify packets to forward

```

```

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

```

```
nx9500-6C8809(config-ip-snmp-acl-SNMPACL)#
```

## Related Commands

|                 |                                            |
|-----------------|--------------------------------------------|
| <code>no</code> | Removes an existing IP access control list |
|-----------------|--------------------------------------------|



### Note

For more information on Access Control Lists, see [ACCESS-LIST](#) on page 1360.

## ipv6

Creates an IPv6 ACL and enters its configuration mode

An IPv6 ACL defines a set of rules that filter IPv6 packets flowing through a port or interface. Each rule specifies the action taken when a packet matches the rule. If the action is deny, the packet is dropped. If the action is permit, the packet is allowed.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
ipv6 access-list <IPv6-ACL-NAME>
```

### Parameters

```
ipv6 access-list <IPv6-ACL-NAME>
```

|                                                |                                                                                                                                                                                                                                        |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>access-list &lt;IPv6-ACL-NAME&gt;</code> | Configures an IPv6 access list and enters its configuration mode <ul style="list-style-type: none"> <li>• <code>&lt;IPv6-ACL-NAME&gt;</code> - Specify the IPv6 ACL name. If the access list does not exist, it is created.</li> </ul> |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```

rfs4000-229D58(config)#ipv6 access-list IPv6ACLTest
rfs4000-229D58(config-ipv6-acl-IPv6ACLTest)#?
IPv6 Access Control Mode commands:
 deny Specify packets to reject
 no Negate a command or set its defaults
 permit Specify packets to forward

 clrscr Clears the display screen

```

```

commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

```

```
rfs4000-229D58(config-ipv6-acl-IPv6ACLTest)#
```

### Related Commands

|                 |                                     |
|-----------------|-------------------------------------|
| <code>no</code> | Removes an IPv6 access control list |
|-----------------|-------------------------------------|



#### Note

For more information on access control lists, see [ACCESS-LIST](#) on page 1360.

### *ipv6-router-advertisement-policy*

Creates an IPv6 RA policy and enters its configuration mode

An IPv6 router policy allows routers to advertise their presence in response to solicitation messages. After receiving a neighbor solicitation message, the destination node sends an advertisement message, which includes the link layer address of the source node. After receiving the advertisement, the destination device replies with a neighbor advertisement message on the local link. After the source receives the advertisement it can communicate with other devices.

Advertisement messages are also sent to indicate a change in link layer address for a node on the local link. With such a change, the multicast address becomes the destination address for advertisement messages.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
ipv6-router-advertisement-policy <POLICY-NAME>
```

#### Parameters

```
ipv6-router-advertisement-policy <POLICY-NAME>
```

|               |                                                                                                    |
|---------------|----------------------------------------------------------------------------------------------------|
| <POLICY-NAME> | Specify an IPv6 RA policy name. If a policy with the specified name does not exist, it is created. |
|---------------|----------------------------------------------------------------------------------------------------|

#### Examples

## Related Commands

|  |
|--|
|  |
|--|

## ipv6-router-advertisement-policy config commands

**Table 24: IPv6 Router Advertisement Policy Config Commands**

| Command                                                  | Description                                                                                                                             |
|----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <code>advertise</code> on page 452                       | Enables advertisement of IPv6 MTU (maximum transmission unit) and hop-count value in RAs                                                |
| <code>assist-neighbor-discovery</code> on page 453       | Enables advertisement of the source link layer address in RAs                                                                           |
| <code>check-ra-consistency</code> on page 453            | Enables checking of consistency in RA values advertised by this router with those advertised by other routers, if any, on the same link |
| <code>dns-server</code> on page 454                      | Configures the DNS server's IPv6 address and lifetime advertised in RAs                                                                 |
| <code>domain-name</code> on page 454                     | Configures the Domain name search label advertised in RAs                                                                               |
| <code>managed-config-flag</code> on page 455             | Sets the managed address configuration flag in RAs                                                                                      |
| <code>nd-reachable-time</code> on page 456               | Enables advertisement of neighbor reachable time in RAs                                                                                 |
| <code>ns-interval</code> on page 457                     | Configures the interval between two successive retransmitted NS (neighbor solicitation) messages                                        |
| <code>other-config-flag</code> on page 457               | Sets the other-configuration flag in RAs                                                                                                |
| <code>ra</code> on page 458                              | Configures RA related parameters, such as the interval between two unsolicited successive RAs                                           |
| <code>router-lifetime</code> on page 459                 | Configures the default router's lifetime, in seconds, advertised in RAs                                                                 |
| <code>router-preference</code> on page 459               | Configures the router preference field value advertised in RAs                                                                          |
| <code>unicast-solicited-advertisement</code> on page 460 | Enables unicasting of solicited RAs                                                                                                     |
| <code>no</code> on page 461                              | Removes or reverts router advertisement policy settings                                                                                 |

### advertise

Enables advertisement of IPv6 MTU and hop-count value in RAs

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
advertise [hop-limit|mtu]
```

### Parameters

```
advertise [hop-limit|mtu]
```

|                                        |                                                                                                            |
|----------------------------------------|------------------------------------------------------------------------------------------------------------|
| <code>advertise [hop-limit mtu]</code> | Enables advertisement of IPv6 MTU and hop-count value in RAs. Both these features are disabled by default. |
|----------------------------------------|------------------------------------------------------------------------------------------------------------|



## Examples

```
nx9500-6C8809(config-ipv6-radv-policy-test)#advertise hop-limit
nx9500-6C8809(config-ipv6-radv-policy-test)#advertise mtu
nx9500-6C8809(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
 advertise mtu
 advertise hop-limit
nx9500-6C8809(config-ipv6-radv-policy-test)#
```

## Related Commands

|                             |                                                               |
|-----------------------------|---------------------------------------------------------------|
| <code>no</code> on page 461 | Disables advertisement of IPv6 MTU and hop-count value in RAs |
|-----------------------------|---------------------------------------------------------------|

## assist-neighbor-discovery

Enables advertisement of the source link layer address in RAs to facilitate neighbor discovery. This feature is enabled by default.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
assist-neighbor-discovery
```

## Parameters

None

## Examples

```
nx9500-6C8809(config-ipv6-radv-policy-test)#assist-neighbor-discovery
```

## Related Commands

|                             |                                                                    |
|-----------------------------|--------------------------------------------------------------------|
| <code>no</code> on page 461 | Disables the advertisement of the source link layer address in RAs |
|-----------------------------|--------------------------------------------------------------------|

## check-ra-consistency

Enables checking of consistency in RA values advertised by this router with those advertised by other routers, if any, on the same link. If the values advertised are inconsistent, a conflict is logged.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
check-ra-consistency
```

## Parameters

None

## Examples

```
nx9500-6C8809(config-ipv6-radv-policy-test)#check-ra-consistency
nx9500-6C8809(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
```

```

advertise mtu
advertise hop-limit
check-ra-consistency
nx9500-6C8809(config-ipv6-radv-policy-test)#

```

#### Related Commands

|                       |                                                                                                                                           |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <b>no</b> on page 461 | Disables comparison of interface-specific parameters advertised by other routers, within the link, with those advertised with this router |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------|

## dns-server

Configures the DNS server's IPv6 address and lifetime. The configured values are advertised in RAs.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
dns-server <IPv6> {lifetime [<4-3600>|expired|infinite]}
```

#### Parameters

```
dns-server <IPv6> {lifetime [<4-3600>|expired|infinite]}
```

|                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dns-server <IPv6>                    | <p>Configures the DNS server's IPv6 address</p> <p>Enables the use of a DNS server to resolve host names to IPv6 addresses. When an IPv6 host is configured with the address of a DNS server, the host sends DNS name queries to the server for resolution.</p> <ul style="list-style-type: none"> <li>• &lt;IPv6&gt; - Specify the DNS server's address. This address is advertised in RAs. A maximum of four (4) entries can be made per policy.</li> </ul> |
| lifetime [<4-3600> expired infinite] | <p>Optional. Configures the DNS server's (identified by the &lt;IPv6&gt; parameter) lifetime</p> <ul style="list-style-type: none"> <li>• &lt;4-3600&gt; - Configures a lifetime in seconds. Specify a value form 4 - 3600 seconds. The default is 600 seconds.</li> <li>• expired - Advertises that this DNS server's lifetime has expired and should not be used</li> <li>• infinite - Advertises that this DNS server's lifetime is infinite</li> </ul>    |

#### Examples

```

nx9500-6C8809(config-ipv6-radv-policy-test)#dns-server 2002::2 lifetime 3000
nx9500-6C8809(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
 advertise mtu
 advertise hop-limit
 check-ra-consistency
 dns-server 2002::2 lifetime 3000
nx9500-6C8809(config-ipv6-radv-policy-test)#

```

#### Related Commands

|                       |                                                                                                         |
|-----------------------|---------------------------------------------------------------------------------------------------------|
| <b>no</b> on page 461 | Removes the DNS server settings advertised in RAs. Once removed these values are not advertised in RAs. |
|-----------------------|---------------------------------------------------------------------------------------------------------|

## domain-name

Configures the Domain name search label advertised in RAs

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
domain-name <WORD> {lifetime [<4-3600>|expired|infinite]}
```

#### Parameters

```
domain-name <WORD> {lifetime [<4-3600>|expired|infinite]}
```

|                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| domain-name <WORD>                   | Configures the Domain name search label advertised in RAs<br>Enter a FQDN (fully qualified domain name), which is an unambiguous domain name available in a router advertisement resource. To distinguish an FQDN from a regular domain name, a trailing period is added. For example, somehost.example.com. <ul style="list-style-type: none"><li>• &lt;WORD&gt; - Specify the Domain name search label. A maximum of four (4) entries can be made per policy.</li></ul> |
| lifetime [<4-3600> expired infinite] | Optional. Configures the Domain name search label's lifetime <ul style="list-style-type: none"><li>• &lt;4-3600&gt; - Configures a lifetime in seconds. Specify a value form 4 - 3600 seconds. The default is 600 seconds.</li><li>• expired - Advertises that this Domain name search label's lifetime has expired and should not be used</li><li>• infinite - Advertises that this Domain name search label's lifetime is infinite</li></ul>                            |

#### Examples

```
nx9500-6C8809(config-ipv6-radv-policy-test)#domain-name TechPubs lifetime infinite
nx9500-6C8809(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
 advertise mtu
 advertise hop-limit
 check-ra-consistency
 dns-server 2002::2 lifetime 3000
 domain-name TechPubs lifetime infinite
nx9500-6C8809(config-ipv6-radv-policy-test)#
```

#### Related Commands

|                       |                                                                                                          |
|-----------------------|----------------------------------------------------------------------------------------------------------|
| <b>no</b> on page 461 | Removes the Domain name settings advertised in RAs. Once removed these values are not advertised in RAs. |
|-----------------------|----------------------------------------------------------------------------------------------------------|

#### managed-config-flag

Sets the managed address configuration flag in RAs. When set, it indicates that IPv6 addresses are available through DHCPv6. This feature is disabled by default.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

managed-config-flag

## Parameters

None

## Examples

```
nx9500-6C8809(config-ipv6-radv-policy-test)#managed-config-flag
nx9500-6C8809(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
managed-config-flag
 advertise mtu
 advertise hop-limit
 check-ra-consistency
 dns-server 2002::2 lifetime 3000
 domain-name TechPubs lifetime infinite
nx9500-6C8809(config-ipv6-radv-policy-test)#
```

## Related Commands

|                |                                                                  |
|----------------|------------------------------------------------------------------|
| no on page 461 | Removes the managed address configuration flag advertised in RAs |
|----------------|------------------------------------------------------------------|

## nd-reachable-time

Enables advertisement of ND (neighbor discovery) reachable time in RAs. This feature is disabled by default.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

nd-reachable-time [<5000-3600000>|global]

## Parameters

nd-reachable-time [<5000-3600000>|global]

|                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| nd-reachable-time<br>[<5000-3600000> global] | Configures the interval, in milliseconds, that a node assumes a neighbor is reachable after receiving a reachability confirmation from the neighbor. Therefore, a neighbor is reachable, after being discovered, for a period specified here. This value is advertised in RAs. Use one of the following options: <ul style="list-style-type: none"><li>• &lt;5000-3600000&gt; - Configures an interface-specific value. Specify a value from 5000 - 3600000 milliseconds. The default is 5000 milliseconds.</li><li>• global - Advertises the neighbor reachable time configured for the system. This is the value configured at the device configuration mode. For more information, see <a href="#">use</a> on page 1232 (profile config mode).</li></ul> |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-ipv6-radv-policy-test)#nd-reachable-time 6000
nx9500-6C8809(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
 managed-config-flag
 nd-reachable-time 6000
 advertise mtu
```

```
advertise hop-limit
check-ra-consistency
dns-server 2002::2 lifetime 3000
domain-name TechPubs lifetime infinite
nx9500-6C8809(config-ipv6-radv-policy-test)#
```

#### Related Commands

|                                |                                                          |
|--------------------------------|----------------------------------------------------------|
| <a href="#">no</a> on page 461 | Disables advertisement of neighbor reachable time in RAs |
|--------------------------------|----------------------------------------------------------|

#### ns-interval

Configures the NS (neighbor solicitation) retransmit timer value advertised in RAs. This is the interval between two successive NS messages. When specified, it enables the sending of the specified value in RAs. This feature is disabled by default.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
ns-interval [<1000-3600000>|global]
```

#### Parameters

```
ns-interval [<1000-3600000>|global]
```

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ns-interval [<1000-3600000> global] | Configures the NS interval advertised in RAs. Use one of the following options: <ul style="list-style-type: none"><li>• &lt;1000-3600000&gt; - Specify a value from 1000 - 3600000 milliseconds. The default is 1000 milliseconds.</li><li>• global - Advertises the NS interval configured for the system. This is configured on the device in the device configuration mode. For more information, see <a href="#">ipv6</a> on page 1162 (profile config mode).</li></ul> |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config-ipv6-radv-policy-test)#ns-interval 3000
nx9500-6C8809(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
managed-config-flag
nd-reachable-time global
ns-interval 3000
advertise mtu
advertise hop-limit
check-ra-consistency
dns-server 2002::2 lifetime 3000
domain-name TechPubs lifetime infinite
nx9500-6C8809(config-ipv6-radv-policy-test)#
```

#### Related Commands

|  |  |
|--|--|
|  |  |
|  |  |
|  |  |
|  |  |

#### other-config-flag

Sets the other-configuration flag in RAs. When set, it indicates that other configuration details, such as DNS-related information, are available through DHCPv6. This feature is enabled by default.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

`other-config-flag`

#### Parameters

None

#### Examples

```
nx9500-6C8809(config-ipv6-radv-policy-test)#other-config-flag
```

#### Related Commands

|                             |                                                 |
|-----------------------------|-------------------------------------------------|
| <code>no</code> on page 461 | Removes the other-config-flag advertised on RAs |
|-----------------------------|-------------------------------------------------|

ra

Configures RA related parameters, such as the interval between two unsolicited successive RAs. It also allows suppression of RAs.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
ra [interval <3-1800>|suppress]
```

#### Parameters

```
ra [interval <3-1800>|suppress]
```

|                   |                                                                                                                                                                                                                                                                                                                         |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| interval <3-1800> | Configures the interval, in seconds, between two unsolicited successive RAs <ul style="list-style-type: none"><li>• &lt;3-1800&gt; - Specify a value from 3 - 1800 seconds. The default is 300 seconds.</li></ul> <p><b>Note:</b> The router-lifetime should be at least three times the specified router interval.</p> |
| suppress          | Enables the suppression of RAs. When enabled, the transmission of RAs in IPv6 packets is suppressed. This option is disabled by default. The <b>no &gt; ra &gt; suppress</b> command enables the sending of RAs.                                                                                                        |

#### Examples

```
nx9500-6C8809(config-ipv6-radv-policy-test)#ra interval 200
nx9500-6C8809(config-ipv6-radv-policy-test)#ra suppress
nx9500-6C8809(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
 ra suppress
 ra interval 200
 managed-config-flag
```

```
nd-reachable-time global
advertise mtu
advertise hop-limit
check-ra-consistency
dns-server 2002::2 lifetime 3000
domain-name TechPubs lifetime infinite
nx9500-6C8809(config-ipv6-radv-policy-test)#
```

#### Related Commands

|                             |                                                         |
|-----------------------------|---------------------------------------------------------|
| <code>no</code> on page 461 | Removes the RA interval, and enables the sending of RAs |
|-----------------------------|---------------------------------------------------------|

### router-lifetime

Configures the default router's lifetime, in seconds, advertised in RAs

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
router-lifetime <0-9000>
```

#### Parameters

```
router-lifetime <0-9000>
```

|                                             |                                                                                                                                                                                                                                                                                             |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>router-lifetime &lt;0-9000&gt;</code> | Configures the default router's lifetime <ul style="list-style-type: none"><li>• <code>&lt;0-9000&gt;</code> – Specify a value from 0 - 9000 seconds. The default value is 1500 seconds.</li></ul> <p><b>Note:</b> A value of "0" indicates that this router is not the default router.</p> |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config-ipv6-radv-policy-test)#router-lifetime 2000
nx9500-6C8809(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
 ra suppress
 ra interval 200
 managed-config-flag
 nd-reachable-time global
 router-lifetime 2000
 advertise mtu
 advertise hop-limit
 check-ra-consistency
 dns-server 2002::2 lifetime 3000
 domain-name TechPubs lifetime infinite
nx9500-6C8809(config-ipv6-radv-policy-test)#
```

#### Related Commands

|                             |                                       |
|-----------------------------|---------------------------------------|
| <code>no</code> on page 461 | Removes the default router's lifetime |
|-----------------------------|---------------------------------------|

### router-preference

Configures the router preference field value advertised in RAs. The options are high, medium, and low. This value is used to prioritize and select the default router when multiple routers are discovered.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
router-preference [high|medium|low]
```

#### Parameters

```
router-preference [high|medium|low]
```

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| router-preference [high medium low] | <p>Sets this router's preference over other routers, in the link, to be the default router. The options are high, low, and medium. The default value is medium. The following points should be taken into consideration when configuring router preference:</p> <ul style="list-style-type: none"><li>• For a router to be selected as a default router, the router's lifetime should not be equal to "0".</li><li>• To enable default router selection, using router information contained in RAs, configure default router selection on that interface.</li></ul> |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config-ipv6-radv-policy-test)#router-preference high
nx9500-6C8809-6C8809(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
 ra suppress
 ra interval 200
 managed-config-flag
 nd-reachable-time global
 router-lifetime 2000
 advertise mtu
 advertise hop-limit
 router-preference high
 check-ra-consistency
 dns-server 2002::2 lifetime 3000
 domain-name TechPubs lifetime infinite
nx9500-6C8809(config-ipv6-radv-policy-test)#
```

#### Related Commands

|                                |                                                             |
|--------------------------------|-------------------------------------------------------------|
| <a href="#">no</a> on page 461 | Removes the router preference field value advertised in RAs |
|--------------------------------|-------------------------------------------------------------|

#### unicast-solicited-advertisement

Enables unicasting of solicited RAs. This feature is disabled by default.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
unicast-solicited-advertisement
```

#### Parameters

None



## Examples

```
nx9500-6C8809(config-ipv6-radv-policy-test)#unicast-solicited-advertisement
nx9500-6C8809(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
 ra suppress
 ra interval 200
 unicast-solicited-advertisement
 managed-config-flag
 nd-reachable-time global
 router-lifetime 2000
 advertise mtu
 advertise hop-limit
 router-preference high
 check-ra-consistency
 dns-server 2002::2 lifetime 3000
 domain-name TechPubs lifetime infinite
nx9500-6C8809(config-ipv6-radv-policy-test)#
```

## Related Commands

|                             |                                      |
|-----------------------------|--------------------------------------|
| <code>no</code> on page 461 | Disables unicasting of solicited RAs |
|-----------------------------|--------------------------------------|

no

Removes or reverts router advertisement policy settings. Use the no command to remove or revert the interface-specific parameters that are advertised by link router.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
no [advertise [hop-limit|mtu]|assist-neighbor-discovery|check-ra-consistency|
dns-server <IPv6>|domain-name <WORD>|managed-config-flag|nd-reachable-time|ns-interval|
other-config-flag|ra [interval|suppress]|router-lifetime|unicast-solicited-advertisement]
```

## Parameters

```
no <PARAMETERS>
```

|                                    |                                                                                                    |
|------------------------------------|----------------------------------------------------------------------------------------------------|
| <code>no &lt;PARAMETERS&gt;</code> | Removes or reverts this IPv6 router advertisement policy's settings based on the parameters passed |
|------------------------------------|----------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
 managed-config-flag
 nd-reachable-time global
 advertise mtu
 advertise hop-limit
 check-ra-consistency
 dns-server 2002::2 lifetime 3000
```

```

domain-name TechPubs lifetime infinite
nx9500-6C8809(config-ipv6-radv-policy-test)#
nx9500-6C8809(config-ipv6-radv-policy-test)#no managed-config-flag
nx9500-6C8809(config-ipv6-radv-policy-test)#no nd-reachable-time
nx9500-6C8809(config-ipv6-radv-policy-test)#no check-ra-consistency
nx9500-6C8809(config-ipv6-radv-policy-test)#show context
ipv6-router-advertisement-policy test
 advertise mtu
 advertise hop-limit
 dns-server 2002::2 lifetime 3000
 domain-name TechPubs lifetime infinite
nx9500-6C8809(config-ipv6-radv-policy-test)#

```

## *l2tpv3*

Configures a L2TPV3 (Layer 2 Tunnel Protocol Version 3) tunnel policy, used to create one or more L2TPV3 tunnels.

The L2TPV3 policy defines the control and encapsulation protocols needed for tunneling layer 2 frames between two IP nodes. This policy enables creation of L2TPV3 tunnels for transporting Ethernet frames between bridge VLANs and physical GE ports. L2TPV3 tunnels can be created between any vendor devices supporting L2TPV3 protocol.

### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### **Syntax**

```
l2tpv3 policy <L2TPV3-POLICY-NAME>
```

### **Parameters**

```
l2tpv3 policy <L2TPV3-POLICY-NAME>
```

|                                       |                                                                                                                                                                                                                                        |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| l2tpv3 policy<br><L2TPV3-POLICY-NAME> | Configures an L2TPV3 tunnel policy <ul style="list-style-type: none"> <li>• &lt;L2TPV3-POLICY-NAME&gt; - Specify a policy name. The policy is created if it does not exist. To modify an existing L2TPV3, specify its name.</li> </ul> |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### **Examples**

```

nx9500-6C8809(config)#l2tpv3 policy L2TPV3Policy1
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#?

```

L2tpv3 Policy Mode commands:

```

cookie-size Size of the cookie field present in each l2tpv3 data
 message
failover-delay Time interval for re-establishing the tunnel after
 the failover (RF-Domain
 manager/VRRP-master/Cluster-master failover)
force-l2-path-recovery Enables force learning of servers, gateways etc.,
 behind the l2tpv3 tunnel when the tunnel is
 established
hello-interval Configure the time interval (in seconds) between
 l2tpv3 Hello keep-alive messages exchanged in l2tpv3
 control connection
no Negate a command or set its defaults
reconnect-attempts Maximum number of attempts to reestablish the

```

```

tunnel.
reconnect-interval Time interval between the successive attempts to
reestablish the l2tpv3 tunnel
retry-attempts Configure the maximum number of retransmissions for
signaling message
retry-interval Time interval (in seconds) before the initiating a
retransmission of any l2tpv3 signaling message
rx-window-size Number of signaling messages that can be received
without sending the acknowledgement
tx-window-size Number of signaling messages that can be sent
without receiving the acknowledgement

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

```

```
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#
```

### Related Commands

|                          |                                          |
|--------------------------|------------------------------------------|
| <code>no</code>          | Removes an existing L2TPV3 tunnel policy |
| <code>mint-policy</code> | Configures the global MiNT policy        |



#### Note

For more information on the L2TPV3 tunnel configuration mode and commands, see [L2TPV3-POLICY](#).

### *location-policy*

Creates a Location policy and enters its configuration mode. Use this command to configure a policy that provides the ExtremeLocation server hostname, and the ExtremeLocation Tenant's API key needed to authenticate and authorize with the server. Apply this Location policy on the WiNG devices (site controller, virtual controllers, and standalone APs). When applied, these devices push/export site hierarchy to the ExtremeLocation server. The site hierarchy includes site details along with details of APs deployed within the site.



#### Note

Once created and configured, apply this Location policy on the WiNG controller's self, to enable Tenant site hierarchy reporting by the controller to the ExtremeLocation server.



#### Note

The ExtremeLocation sensor capabilities are supported only on AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP8432, AP8533 model access points.

### Supported in the following platforms:

- Access Points — AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 8432, AP 8533
- Wireless Controllers — RFS 4000

- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
location-policy <LOCATION-POLICY-NAME>
```

## Parameters

```
location-policy <LOCATION-POLICY-NAME>
```

|                                        |                                                                                                      |
|----------------------------------------|------------------------------------------------------------------------------------------------------|
| location-policy <LOCATION-POLICY-NAME> | Specify the Location Policy name. If a policy with the specified name does not exist, it is created. |
|----------------------------------------|------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config)#eloc-policy testLocPolicy
nx9500-6C8809(config-eloc-policy-testLocPolicy)#?
Eloc Policy Mode commands:
 enable Enable this eloc policy
 location-key API key used for location service
 no Negate a command or set its defaults
 server-host ExtremeLocation server configuration

 clrscr Clears the display screen
 commit Commit all changes made in this session
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-eloc-policy-testLocPolicy)#
```

## Related Commands

|                                                     |                                                     |
|-----------------------------------------------------|-----------------------------------------------------|
| <a href="#">no (global-config-mode)</a> on page 475 | Removes an existing Location policy from the system |
|-----------------------------------------------------|-----------------------------------------------------|

## location-policy-config-mode commands

The following table summarizes the Location Policy configuration commands:

**Table 25: Location Policy Config Mode Commands**

| Command                                  | Description                                                                                                                               |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">enable</a> on page 464       | Enables the location policy                                                                                                               |
| <a href="#">location-key</a> on page 465 | Configures the ExtremeLocation Tenant's API key. This key is used by the WiNG controller to authenticate with the ExtremeLocation server. |
| <a href="#">server-host</a> on page 466  | Configures the ExtremeLocation server's hostname                                                                                          |
| <a href="#">no</a> on page 466           | Removes Location policy settings or reverts them to default values                                                                        |

enable

Enables this Location policy

Supported in the following platforms:

- Access Points — AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

`enable`

#### Parameters

None

#### Examples

```
nx9500-6C8809(config-location-policy-ELocPolicy)#enable
nx9500-6C8809(config-location-policy-ELocPolicy)#show context
location-policy ELocPolicy
 enable
nx9500-6C8809(config-location-policy-ELocPolicy)#
```

#### Related Commands

|                             |                               |
|-----------------------------|-------------------------------|
| <code>no</code> on page 466 | Disables this Location policy |
|-----------------------------|-------------------------------|

### location-key

Configures the ExtremeLocation Tenant's API key. The WiNG controller uses this key to authenticate with the ExtremeLocation server, and stage the Tenant's site hierarchy (includes site details and details of AP deployed within the site).

Supported in the following platforms:

- Access Points — AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

`location-key <API-KEY>`

#### Parameters

`location-key <API-KEY>`

|                                           |                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>location-key &lt;API-KEY&gt;</code> | <p>Enter the 64-bit key that the WiNG controller uses to authenticate with the ExtremeLocation server.</p> <ul style="list-style-type: none"> <li>• <code>&lt;API-KEY&gt;</code> - Enter the key.</li> </ul> <p><b>Note:</b> To generate API-Key, log into your ExtremeLocation Tenant account and use the ExtremeLocation UI. Enter that key here in the Location Policy.</p> |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config-location-policy-ELocPolicy)#location-key dGVzdEAXmJmONQo
nx9500-6C8809(config-location-policy-ELocPolicy)#show context
location-policy ELocPolicy
 enable
 location-key dGVzdEAXmJmONQo
nx9500-6C8809(config-location-policy-ELocPolicy)#
```

#### Related Commands

|                             |                                                       |
|-----------------------------|-------------------------------------------------------|
| <code>no</code> on page 466 | Removes the Tenant's API-Key from the Location policy |
|-----------------------------|-------------------------------------------------------|

## server-host

Configures the ExtremeLocation server's hostname. When configured, the WING controller stages the Tenant's site hierarchy information to the specified server.

Supported in the following platforms:

- Access Points — AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
server-host 1 ip <HOSTNAME> {port <1-65535>}
```

### Parameters

```
server-host 1 ip <HOSTNAME> {port <1-65535>}
```

|                                |                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| server-host 1 ip<br><HOSTNAME> | Identifies the ExtremeLocation server by its hostname <ul style="list-style-type: none"><li>• &lt;HOSTNAME&gt; - Enter ExtremeLocation server's hostname.</li></ul> <p><b>Note:</b> Enter the server's hostname and not the IP address, as the IP address is likely to change periodically in order to balance load across multiple Location server instances.</p> |
| {port <1-65535>}               | optional. Configures the port on which the ExtremeLocation server is reachable <ul style="list-style-type: none"><li>• &lt;1-63335&gt; - Selects a port from 1 - 65535 for the ExtremeLocation server.</li></ul> <p><b>Note:</b> By default the ExtremeLocation server is reachable on port 443.</p>                                                               |

### Examples

```
nx9500-6C8809(config-location-policy-ELocPolicy)#server-host 1 ip xyz.com
nx9500-6C8809(config-location-policy-ELocPolicy)#show context
location-policy ELocPolicy
 enable
 server-host 1 ip xyz.com port 443
 location-key dGVzdEAxMjM0NQo
nx9500-6C8809(config-location-policy-ELocPolicy)#
```

### Related Commands

|                |                                                           |
|----------------|-----------------------------------------------------------|
| no on page 466 | Removes ExtremeLocation server's hostname from the policy |
|----------------|-----------------------------------------------------------|

## no

Removes this Location Policy settings or reverts them to default values

Supported in the following platforms:

- Access Points — AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
no [enable|location-key|server-host]
```

### Parameters

```
no <PARAMETERS>
```

```
no <PARAMETERS>
```

Removes this Location Policy settings or reverts to default values, based on the parameters passed

## Examples

The following example shows the 'ELocPolicy' policy settings before the 'no' commands were executed:

```
nx9500-6C8809(config-location-policy-ELocPolicy)#show context
location-policy ELocPolicy
 enable
 server-host 1 ip xyz.com port 443
 location-key dGVzdEAxMjM0NzQ=
nx9500-6C8809(config-location-policy-ELocPolicy)#
nx9500-6C8809(config-location-policy-ELocPolicy)#no server-host 1
nx9500-6C8809(config-location-policy-ELocPolicy)#no enable
nx9500-6C8809(config-location-policy-ELocPolicy)#no location-key
```

The following example shows the 'ELocPolicy' policy settings after the 'no' commands were executed:

```
nx9500-6C8809(config-location-policy-ELocPolicy)#show context
location-policy ELocPolicy
nx9500-6C8809(config-location-policy-ELocPolicy)#
```

## mac

Configures a MAC ACL

Access lists define access permissions to the network using a set of rules. Each rule specifies an action taken when a packet matches the rule. If the action is deny, the packet is dropped. If the action is permit, the packet is allowed.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
mac access-list <MAC-ACL-NAME>
```

### Parameters

```
mac access-list <MAC-ACL-NAME>
```

```
access-list <IP-ACL-NAME>
```

Configures a MAC access control list

- <MAC-ACL-NAME> – Specify the ACL name. If a MAC ACL with the specified name does not exist, it is created.

### Examples

```
nx9500-6C8809(config)#mac access-list test
nx9500-6C8809(config-mac-acl-test)#?
MAC Extended ACL Configuration commands:
 deny Specify packets to reject
 disable Disable rule if not needed
 ex3500 Ex3500 device
 insert Insert this rule (instead of overwriting a existing rule)
 no Negate a command or set its defaults
```

```

permit Specify packets to forward

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

```

```
nx9500-6C8809(config-mac-acl-test)#
```

## Related Commands

|                 |                                             |
|-----------------|---------------------------------------------|
| <code>no</code> | Removes an existing MAC access control list |
|-----------------|---------------------------------------------|



### Note

For more information on Access Control Lists, see.

## *management-policy*

Configures a management policy. Management policies include services that run on a device, welcome messages, banners, etc.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
management-policy <MANAGEMENT-POLICY-NAME>
```

### Parameters

```
management-policy <MANAGEMENT-POLICY-NAME>
```

|                                             |                                                                                  |
|---------------------------------------------|----------------------------------------------------------------------------------|
| <code>&lt;MANAGEMENT-POLICY-NAME&gt;</code> | Specify the management policy name. If the policy does not exist, it is created. |
|---------------------------------------------|----------------------------------------------------------------------------------|

### Examples

```

nx9500-6C8809(config)#management-policy test
nx9500-6C8809(config-management-policy-test)#?
Management Mode commands:
 aaa-login Set authentication for logins
 allowed-locations Add allowed locations
 banner Define a login banner
 ftp Enable FTP server
 http Hyper Text Terminal Protocol (HTTP)
 https Secure HTTP
 idle-session-timeout Configure idle timeout for a configuration session
 (GUI or CLI)
 ipv6 IPv6 management access restriction

```



|                         |                                                         |
|-------------------------|---------------------------------------------------------|
| no                      | Negate a command or set its defaults                    |
| passwd-retry            | Lockout user if too many consecutive login failures     |
| privilege-mode-password | Set the password for entering CLI privilege mode        |
| rest-server             | Enable rest server for device on-boarding functionality |
| restrict-access         | Restrict management access to the device                |
| snmp-server             | SNMP                                                    |
| ssh                     | Enable ssh                                              |
| t5                      | T5 configuration                                        |
| telnet                  | Enable telnet                                           |
| user                    | Add a user account                                      |
| clrscr                  | Clears the display screen                               |
| commit                  | Commit all changes made in this session                 |
| do                      | Run commands from Exec mode                             |
| end                     | End current mode and change to EXEC mode                |
| exit                    | End current mode and down to previous mode              |
| help                    | Description of the interactive help system              |
| revert                  | Revert changes                                          |
| service                 | Service Commands                                        |
| show                    | Show running system information                         |
| write                   | Write running configuration to memory or terminal       |

nx9500-6C8809(config-management-policy-test)#

### Related Commands

|    |                                       |
|----|---------------------------------------|
| no | Removes an existing management policy |
|----|---------------------------------------|



#### Note

For more information on Management policy configuration, see [MANAGEMENT-POLICY](#).

### *meshpoint*

Creates a new meshpoint and enters its configuration mode. Use this command to select and configure existing meshpoints.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
meshpoint [<MESHPOINT-NAME>|containing <WORD>]
```

#### Parameters

```
meshpoint [<MESHPOINT-NAME>|containing <WORD>]
```

|                   |                                                                             |
|-------------------|-----------------------------------------------------------------------------|
| <MESHPOINT-NAME>  | Specify the meshpoint name. If the meshpoint does not exist, it is created. |
| containing <WORD> | Selects existing meshpoints containing the sub-string <WORD> in their names |

## Examples

```
nx9500-6C8809(config)#meshpoint testMeshpoint
nx9500-6C8809(config-meshpoint-testMeshpoint)#?
Mesh Point Mode commands:
 allowed-vlans Set the allowed VLANs
 beacon-format The beacon format of this meshpoint
 control-vlan VLAN for meshpoint control traffic
 data-rates Specify the 802.11 rates to be supported on this meshpoint
 description Configure a description of the usage of this meshpoint
 force Force suboptimal paths
 meshid Configure the Service Set Identifier for this meshpoint
 neighbor Configure neighbor specific parameters
 no Negate a command or set its defaults
 root Set this meshpoint as root
 security-mode The security mode of this meshpoint
 shutdown Shutdown this meshpoint
 use Set setting to use
 wpa2 Modify ccmp wpa2 related parameters

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-meshpoint-testMeshpoint)#
```

## Related Commands

|                 |                               |
|-----------------|-------------------------------|
| <code>no</code> | Removes an existing meshpoint |
|-----------------|-------------------------------|



### Note

For more information on Meshpoint configuration, see [MESHPOINT](#).

## *meshpoint-qos-policy*

Configures a set of parameters that defines the meshpoint QoS policy

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
meshpoint-qos-policy <MESHPOINT-QOS-POLICY-NAME>
```

### Parameters

```
meshpoint-qos-policy <MESHPOINT-QOS-POLICY-NAME>
```

|                             |                                                                                                           |
|-----------------------------|-----------------------------------------------------------------------------------------------------------|
| <MESHPOINT-QOS-POLICY-NAME> | Specify the meshpoint QoS policy name. If a policy with the specified name does not exist, it is created. |
|-----------------------------|-----------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config)#meshpoint-qos-policy test
nx9500-6C8809(config-meshpoint-qos-test)#?
Mesh Point QoS Mode commands:
 accelerated-multicast Configure accelerated multicast streams address and
 forwarding QoS classification
 no Negate a command or set its defaults
 rate-limit Configure traffic rate-limiting parameters on a
 per-meshpoint/per-neighbor basis

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-meshpoint-qos-test)#
```

### Related Commands

|    |                                          |
|----|------------------------------------------|
| no | Removes an existing meshpoint QoS policy |
|----|------------------------------------------|



#### Note

For more information on Meshpoint QoS policy configuration, see [MESHPOINT](#).

### *mint-policy*

Configures the global MiNT policy

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
mint-policy global-default
```

#### Parameters

```
mint-policy global-default
```

|                |                                           |
|----------------|-------------------------------------------|
| global-default | Configures the global default MiNT policy |
|----------------|-------------------------------------------|

## Examples

```
nx9500-6C8809(config)#mint-policy global-default
nx9500-6C8809(config-mint-policy-global-default)#?
Mint Policy Mode commands:
 level Mint routing level
 lsp LSP
 mtu Configure the global Mint MTU
 no Negate a command or set its defaults
 router Mint router
 udp Configure mint UDP/IP encapsulation

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-mint-policy-global-default)#
```



### Note

For more information on MiNT policy configuration, see [MINT-POLICY](#) on page 1513.

## *nac-list*

Configures a NAC (Network Access Control) list that manages access to the network

A NAC list configures a list of devices that can access a network based on their MAC addresses.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
nac-list <NAC-LIST-NAME>
```

### Parameters

```
nac-list <NAC-LIST-NAME>
```

|                                                                                                                 |
|-----------------------------------------------------------------------------------------------------------------|
| <NAC-LIST-NAME> Specify the NAC list name. If a NAC list with the specified name does not exist, it is created. |
|-----------------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config)#nac-list test
nx9500-6C8809(config-nac-list-test)#?
NAC List Mode commands:
 exclude Specify MAC addresses to be excluded from the NAC enforcement list
 include Specify MAC addresses to be included in the NAC enforcement list
 no Negate a command or set its defaults
```

```

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

```

```
nx9500-6C8809(config-nac-list-test)#
```

### Related Commands

|                 |                              |
|-----------------|------------------------------|
| <code>no</code> | Removes an existing NAC list |
|-----------------|------------------------------|

### nac-list-mode-commands

The following table summarizes NAC list configuration mode commands:

Table: NAC-List Config Mode Commands

| Command              | Description                                                        |
|----------------------|--------------------------------------------------------------------|
| <code>exclude</code> | Specifies the MAC addresses excluded from the NAC enforcement list |
| <code>include</code> | Specifies the MAC addresses included in the NAC enforcement list   |
| <code>no</code>      | Cancels an exclude or include NAC list rule                        |

#### exclude

Specifies the MAC addresses excluded from the NAC enforcement list

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
exclude <START-MAC> [<END-MAC> precedence <1-1000>|precedence <1-1000>]
```

#### Parameters

```
exclude <START-MAC> [<END-MAC> precedence <1-1000>|precedence <1-1000>]
```

|                        |                                                                                                                                                                                                                                                                                               |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <START-MAC>            | Specifies a range of MAC addresses or a single MAC address to exclude from the NAC enforcement list <ul style="list-style-type: none"> <li>&lt;START-MAC&gt; – Specify the first MAC address in the range.</li> </ul> <p><b>Note:</b> Use this parameter to specify a single MAC address.</p> |
| <END-MAC>              | Specifies the last MAC address in the range (optional if a single MAC is added to the list) <ul style="list-style-type: none"> <li>&lt;END-MAC&gt; – Specify the last MAC address in the range.</li> </ul>                                                                                    |
| precedence<br><1-1000> | Sets the rule precedence. Exclude entries are checked in the order of their rule precedence. <ul style="list-style-type: none"> <li>&lt;1-1000&gt; – Specify a value from 1 - 1000.</li> </ul>                                                                                                |

### Examples

```

nx9500-6C8809(config-nac-list-test)#exclude 00-40-96-B0-BA-2A precedence 1
nx9500-6C8809(config-nac-list-test)#show context
nac-list test
 exclude 00-40-96-B0-BA-2A 00-40-96-B0-BA-2A precedence 1
nx9500-6C8809(config-nac-list-test)#

```

### Related Commands

|           |                                            |
|-----------|--------------------------------------------|
| <b>no</b> | Removes an exclude rule from this NAC list |
|-----------|--------------------------------------------|

### include

Specifies the MAC addresses included in the NAC enforcement list

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
include <START-MAC> [<END-MAC> precedence <1-1000>|precedence <1-1000>]
```

### Parameters

```
include <START-MAC> [<END-MAC> precedence <1-1000>|precedence <1-1000>]
```

|                        |                                                                                                                                                                                                                                                                                             |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <START-MAC>            | Specifies a range of MAC addresses or a single MAC address to include in the NAC enforcement list <ul style="list-style-type: none"> <li>&lt;START-MAC&gt; – Specify the first MAC address in the range.</li> </ul> <p><b>Note:</b> Use this parameter to specify a single MAC address.</p> |
| <END-MAC>              | Specifies the last MAC address in the range (optional if a single MAC is added to the list) <ul style="list-style-type: none"> <li>&lt;END-MAC&gt; – Specify the last MAC address in the range.</li> </ul>                                                                                  |
| precedence<br><1-1000> | Sets the rule precedence. Include entries are checked in the order of their rule precedence. <ul style="list-style-type: none"> <li>&lt;1-1000&gt; – Specify a value from 1 - 1000.</li> </ul>                                                                                              |

### Examples

```

nx9500-6C8809(config-nac-list-test)#include 00-15-70-38-06-49 precedence 2
nx9500-6C8809(config-nac-list-test)#show context
nac-list test

```

```
exclude 00-04-96-B0-BA-2A 00-04-96-B0-BA-2A precedence 1
include 00-15-70-38-06-49 00-15-70-38-06-49 precedence 2
nx9500-6C8809(config-nac-list-test)#
```

#### Related Commands

|    |                                            |
|----|--------------------------------------------|
| no | Removes an include rule from this NAC list |
|----|--------------------------------------------|

#### no (nac-config-mode)

Cancels an exclude or include NAC list rule

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
no [exclude|include]
no [exclude|include] <START-MAC> [<END-MAC> precedence <1-1000>|precedence <1-1000>]
```

#### Parameters

```
no <PARAMETERS>
```

|                 |                                                                            |
|-----------------|----------------------------------------------------------------------------|
| no <PARAMETERS> | Removes or reverts this NAC list's settings based on the parameters passed |
|-----------------|----------------------------------------------------------------------------|

#### Examples

The following example shows the NAC list 'test' settings before the 'no' command is executed:

```
nx9500-6C8809(config-nac-list-test)#show context
nac-list test
 exclude 00-04-96-B0-BA-2A 00-04-96-B0-BA-2A precedence 1
 include 00-15-70-38-06-49 00-15-70-38-06-49 precedence 2
nx9500-6C8809(config-nac-list-test)#
nx9500-6C8809(config-nac-list-test)#no exclude 00-40-96-B0-BA-2A precedence 1
```

The following example shows the NAC list 'test' settings after the 'no' command is executed:

```
nx9500-6C8809(config-nac-list-test)#show context
nac-list test
 include 00-15-70-38-06-49 00-15-70-38-06-49 precedence 2
nx9500-6C8809(config-nac-list-test)#
```

#### no (global-config-mode)

Negates a command, or reverts configured settings to their default

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
no [aaa-policy|aaa-tacacs-policy|alias|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|
ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap8432|ap8533|nx5500|nx75xx|nx9000|nx9600|
application|application-group|application-policy|association-acl-policy|auto-provisioning-
policy|
bgp|bonjour-gw-discovery-policy|bonjour-gw-forwarding-policy|bonjour-gw-query-forwarding-
policy|
captive-portal|client-identity|client-identity-group|crypto-cmp-policy|customize|
database-policy|device|device-categorization|dhcp-server-policy|dhcpv6-server-policy|
dns-whitelist|event-system-policy|ex3500|ex3500-management-policy|ex3500-qos-class-map-
policy|
ex3500-qos-policy-map|ex3524|ex3548|firewall-policy|global-association-list|guest-
management|
igmp-snoop-policy|inline-password-encryption|iot-device-type-imagotag-policy|ip|ipv6|
ipv6-router-advertisement-policy|l2tpv3|location-policy|mac|management-policy|meshpoint|
meshpoint-qos-policy|nac-list|nsight-policy|passpoint-policy|password-encryption|profile|
radio-qos-policy|radius-group|radius-server-policy|radius-user-pool-policy|rf-domain|
rfs4000|roaming-assist-policy|role-policy|route-map|routing-policy|rtl-server-policy|
schedule-policy|t5|sensor-policy|smart-rf-policy|url-filter|url-list|vx9000|
web-filter-policy|wips-policy|wlan|wlan-qos-policy|service]
no alias [address-range <ADDRESS-RANGE-ALIAS-NAME>|host <HOST-ALIAS-NAME>|
network <NETWORK-ALIAS-NAME>|network-group <NETWORK-GROUP-ALIAS-NAME> [address-range|host|
network]]
network-service <NETWORK-SERVICE-ALIAS-NAME>|number <NUMBER-ALIAS-NAME>|string <STRING-
ALIAS-NAME>|
vlan <VLAN-ALIAS-NAME>]
no [aaa-policy|aaa-tacacs-policy|application-policy|auto-provisioning-policy|
auto-provisioning-policy|bonjour-gw-discovery-policy|bonjour-gw-forwarding-policy|
bonjour-gw-query-forwarding-policy|database-policy|captive-portal|crypto-cmp-policy|
device-categorization|dhcp-server-policy|dhcpv6-server-policy|dns-whitelist|event-system-
policy|
ex3500|ex3500-management-policy|ex3500-qos-class-map-policy|ex3500-qos-policy|firewall-
policy|
global-association-list|guest-management|igmp-snoop-policy|inline-password-encryption|ip|
ipv6|
iot-device-type-imagotag-policy|ipv6-router-advertisement-policy|l2tpv3|location-policy|
mac|management-policy|meshpoint|meshpoint-qos-policy|nac-list|nsight-policy|passpoint-
policy|
radio-qos-policy|radius-group|radius-server-policy|radius-user-pool-policy|roaming-assist-
policy|
role-policy|routing-policy|rtl-server-policy|schedule-policy|sensor-policy|smart-rf-policy|
web-filter-policy|wips-policy|wlan-qos-policy] <POLICY-NAME>
no application <APPLICATION-NAME>
no application-group <APPLICATION-GROUP-NAME>
no [ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|
ap81xx|ap8432|ap8533|ex3524|ex3548|rfs4000|t5|nx5500|nx75xx|nx9000|nx9600|vx9000] <MAC>
no client-identity <CLIENT-IDENTITY-NAME>
no client-identity-group <CLIENT-IDENTITY-GROUP-NAME>
no device {containing <WORD>} {(filter type [ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|
ap7562|ap8163|ap8432|ap8533|ex3524|ex3548|rfs4000|t5|nx5500|nx75xx|nx9000|nx9600|vx9000])}
no customize [hostname-column-width|show-wireless-client|show-wireless-client-stats|
show-wireless-client-stats-rf|show-wireless-meshpoint|show-wireless-meshpoint-neighbor-
stats|
show-wireless-meshpoint-neighbor-stats-rf|show-wireless-radio|show-wireless-radio-stats|
show-wireless-radio-stats-rf]
no password-encryption secret 2 <OLD-PASSPHRASE>
no profile {ap6522|ap71xx|ap7502|ap7522|ap7532|ap7562|ap8163|ap8432|ap8533|ex3524|
ex3548|containing|filter|rfs4000|nx5500|nx75xx|nx9000|nx9600|t5|vx9000} <PROFILE-NAME>
no wlan [<WLAN-NAME>|all|containing <WLAN-NAME-SUBSTRING>]
no service set [command-history|reboot-history|upgrade-history] {on <DEVICE-NAME>}
```



The following 'no' commands are specific to the NX 9500 and NX 9600 platforms:

```
no t5 <T5-DEVICE-MAC>
no bgp [as-path-list|community-list|extcommunity-list|ip-access-list|ip-prefix-list] <LIST-NAME>
```

The following 'no' commands are specific to the NX 9500 and NX 9600 platforms:

```
no route-map <ROUTE-MAP-NAME>
```

The following 'no' commands are specific to the AP 6522, AP 6532, AP 7161, AP 7502, AP 7522, AP 7532, and RFS 4000 platforms:

```
no url-filter <URL-FILTER-NAME>
no url-list <URL-LIST-NAME>
no web-filter-name <WEB-FILTER-NAME>
```

The following 'no' command is specific to the VX 9000 virtual machine platform:

```
no database-client-policy <POLICY-NAME>
```

## Parameters

```
no <PARAMETERS>
```

|                 |                                                                                                           |
|-----------------|-----------------------------------------------------------------------------------------------------------|
| no <PARAMETERS> | Removes or resets settings, configurable in the global configuration mode, based on the parameters passed |
|-----------------|-----------------------------------------------------------------------------------------------------------|

## Examples

```
<DEVICE>(config)#no ?
aaa-policy Delete a aaa policy
aaa-tacacs-policy Delete a aaa tacacs policy
alias Alias
ap621 Delete an AP621 access point
ap622 Delete an AP622 access point
ap650 Delete an AP650 access point
ap6511 Delete an AP6511 access point
ap6521 Delete an AP6521 access point
ap6522 Delete an AP6522 access point
ap6532 Delete an AP6532 access point
ap6562 Delete an AP6562 access point
ap71xx Delete an AP71XX access point
ap7502 Delete an AP7502 access point
ap7522 Delete an AP7522 access point
ap7532 Delete an AP7532 access point
ap7562 Delete an AP7562 access point
ap7602 Delete an AP7602 access point
ap7612 Delete an AP7612 access point
ap7622 Delete an AP7622 access point
ap7632 Delete an AP7632 access point
ap7662 Delete an AP7662 access point
ap81xx Delete an AP81XX access point
ap82xx Delete an AP82XX access point
ap8432 Delete an AP8432 access point
ap8533 Delete an AP8533 access point
application Delete an application
application-group Delete an application-group
application-policy Delete an application policy
association-acl-policy Delete an association-acl policy
auto-provisioning-policy Delete an auto-provisioning policy
bgp BGP Configuration
bonjour-gw-discovery-policy Disable Bonjour Gateway discovery policy
bonjour-gw-forwarding-policy Disable Bonjour Gateway Forwarding policy
```

|                                    |                                                                       |
|------------------------------------|-----------------------------------------------------------------------|
| bonjour-gw-query-forwarding-policy | Disable Bonjour Gateway Query Forwarding policy                       |
| captive-portal                     | Delete a captive portal                                               |
| client-identity                    | Client identity (DHCP Device Fingerprinting)                          |
| client-identity-group              | Client identity group (DHCP Fingerprint Database)                     |
| crypto-cmp-policy                  | CMP policy                                                            |
| customize                          | Restore the custom cli commands to default                            |
| database-client-policy             | Configure database policy                                             |
| database-policy                    | Configure database policy                                             |
| device                             | Delete multiple devices                                               |
| device-categorization              | Delete device categorization object                                   |
| dhcp-server-policy                 | DHCP server policy                                                    |
| dhcpv6-server-policy               | DHCPv6 server related configuration                                   |
| dns-whitelist                      | Delete a whitelist object                                             |
| event-system-policy                | Delete a event system policy                                          |
| ex3500                             | Ex3500 device                                                         |
| ex3500-management-policy           | Delete a ex3500 management policy                                     |
| ex3500-qos-class-map-policy        | Delete a ex3500 qos class-map policy                                  |
| ex3500-qos-policy-map              | Delete a ex3500 qos policy-map                                        |
| ex3524                             | Delete an EX3524 wireless controller                                  |
| ex3548                             | Delete an EX3548 wireless controller                                  |
| firewall-policy                    | Configure firewall policy                                             |
| global-association-list            | Delete a global association list                                      |
| guest-management                   | Delete a guest management policy                                      |
| igmp-snoop-policy                  | Remove device onboard igmp snoop policy                               |
| inline-password-encryption         | Disable storing encryption key in the startup configuration file      |
| iot-device-type-imagotag-policy    | Delete a iot imagotag policy                                          |
| ip                                 | Internet Protocol (IP)                                                |
| ipv6                               | Internet Protocol version 6 (IPv6)                                    |
| ipv6-router-advertisement-policy   | IPv6 Router Advertisement related configuration                       |
| l2tpv3                             | Negate a command or set its defaults                                  |
| location-policy                    | Delete a ExtremeLocation policy                                       |
| mac                                | MAC configuration                                                     |
| management-policy                  | Delete a management policy                                            |
| meshpoint                          | Delete a meshpoint object                                             |
| meshpoint-qos-policy               | Delete a mesh point QoS configuration policy                          |
| nac-list                           | Delete an network access control list                                 |
| nsight-policy                      | Delete a nsight policy                                                |
| nx45xx                             | Delete an NX45XX integrated services platform                         |
| nx5500                             | Delete an NX5500 wireless controller                                  |
| nx65xx                             | Delete an NX65XX integrated services platform                         |
| nx75xx                             | Delete an NX75XX wireless controller                                  |
| nx9000                             | Delete an NX9000 wireless controller                                  |
| passpoint-policy                   | Delete a passpoint configuration policy                               |
| password-encryption                | Disable password encryption in configuration                          |
| profile                            | Delete a profile and all its associated configuration                 |
| radio-qos-policy                   | Delete a radio QoS configuration policy                               |
| radius-group                       | Local radius server group configuration                               |
| radius-server-policy               | Remove device onboard radius policy                                   |
| radius-user-pool-policy            | Configure Radius User Pool                                            |
| rf-domain                          | Delete one or more RF-domains and all their associated configurations |
| rfs4000                            | Delete an RFS4000 wireless controller                                 |
| rfs6000                            | Delete an RFS6000 wireless controller                                 |

|                       |                                                |
|-----------------------|------------------------------------------------|
| rfs7000               | Delete an RFS7000 wireless controller          |
| roaming-assist-policy | Delete a roaming-assist policy                 |
| role-policy           | Role based firewall policy                     |
| route-map             | Dynamic routing route map Configuration        |
| routing-policy        | Policy Based Routing Configuration             |
| rtl-server-policy     | Delete a rtl server policy                     |
| schedule-policy       | Delete a schedule policy                       |
| sensor-policy         | Delete a sensor policy                         |
| smart-rf-policy       | Delete a smart-rf-policy                       |
| t5                    | Delete an T5 DSL switch                        |
| url-filter            | Delete a url filter                            |
| url-list              | Delete a URL list                              |
| vx9000                | Delete an VX9000 wireless controller           |
| web-filter-policy     | Delete a web filter policy                     |
| wips-policy           | Delete a wips policy                           |
| wlan                  | Delete a wlan object                           |
| wlan-qos-policy       | Delete a wireless lan QoS configuration policy |
| service               | Service Commands                               |

<DEVICE>(config)#

### *nsight-policy (global-config-mode)*

Creates an NSight policy and enters its configuration mode

The NSight policy is an advance management, analytics, reporting, and troubleshooting tool, which when created and applied at the RF Domain level allows the RF Domain manager to send statistics (polled from devices within the RF Domain) to the NOC. The NOC, when enabled as the NSight server, stores this data in a locally or externally hosted database. This large, complex data is collated and presented on an NSight Dashboard that can be launched from the NSight-enabled NOC. For large networks, enabling NSight removes the inadequacies of the existing data collection, presentation, and analytics framework. It simplifies network monitoring, troubleshooting, and reporting.



#### **Note**

NSight is a licensed feature, and can be enabled only on the application of an NSight license in the NSight server's self mode.

The NSight features include:

- Network statistic and event visualization - Simplified and unified network views based on defined user roles
- Custom dashboards - Live network health information in real-time to optimally assist network administrators
- Live troubleshooting tools - Packet capture, wireless debug logs, TCP/IP ping and traceroute
- Interactive floor maps with timeline views - Visualize and identify potential issues and problems areas
- Real-time trend analysis - Simplify network growth planning
- Exceptionally responsive interface - Any information the admin needs is three, or less, clicks away

The WiNG NSight implementation consists of the following components:

- An NSight server
- A database. This database consists of AP statistics gathered by RF Domain managers.
- An NSight UI portal

- An NSight client hosted on the RF Domain manager, which periodically gathers statistics from APs and forwards to the NSight server.
- Event history – Event details for all APs adopted by the NOC. These are events received by the Cfgd every 30 seconds and sent to the MART server. Each event consists of the RF Domain name, wireless client MAC if applicable, AP MAC, event mnemonic, event timestamp, and the event string itself.

#### Supported in the following platforms:

- Service Platforms — NX 95XX, NX 96XX, VX 9000

#### Syntax

```
nsight-policy <NSIGHT-POLICY-NAME>
```

#### Parameters

```
nsight-policy <NSIGHT-POLICY-NAME>
```

|                      |                                                                              |
|----------------------|------------------------------------------------------------------------------|
| <NSIGHT-POLICY-NAME> | Specify the NSight policy name. If the policy does not exist, it is created. |
|----------------------|------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config)#nsight-policy test
nx9500-6C8809(config-nsight-policy-test)#?
Nsight Policy Mode commands:
 enable Enable this Nsight policy
 event-history-size Size of the event history collection
 history-ttl Time to live for historical data
 mandatory Configure mandatory app stats reporting
 no Negate a command or set its defaults
 nsight-server Enable Nsight server functionality
 server Configure Nsight server

 clrscr Clears the display screen
 commit Commit all changes made in this session
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-nsight-policy-test)#
```

#### Related Commands

|    |                                   |
|----|-----------------------------------|
| no | Removes an existing NSight policy |
|----|-----------------------------------|

#### nsight-policy config commands

The following table summarizes NSight policy configuration mode commands:

**Table 26: NSight-Policy Config Mode Commands**

| Command                                     | Description                                                                                                            |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| <code>enable</code> on page 481             | Enables this NSight policy                                                                                             |
| <code>event-history-size</code> on page 481 | Converts and sizes the NSight event history collection to a capped collection                                          |
| <code>history-ttl</code> on page 482        | Configures the TTL, in days, for historical data related to clients and devices                                        |
| <code>mandatory</code> on page 482          | Enables mandatory AVC (Application Visibility and Control) statistics reporting                                        |
| <code>nsight-server</code> on page 484      | Enables NSight server functionality and configures the SMTP report delivery settings                                   |
| <code>server</code> on page 485             | Configures the NSight server host. This configuration is used by the NSight client to identify the NSight server host. |
| <code>no</code> on page 485                 | Removes this NSight policy settings                                                                                    |

### enable

Enables this NSight policy. The default setting is enabled.

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 96XX, VX 9000

#### Syntax

`enable`

#### Parameters

`enable`

#### Examples

```
nx9510-6C8A5C(config-nsight-policy-test2)#enable
```

#### Related Commands

|                             |                             |
|-----------------------------|-----------------------------|
| <code>no</code> on page 485 | Disables this NSight policy |
|-----------------------------|-----------------------------|

### event-history-size

Converts and sizes the NSight event history collection to a capped collection. The conversion occurs when upgrading. Use this command to define the NSight event history collection's size and prevent its unbounded growth. Note, resizing the collection results in the collection contents being dropped.

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 96XX, VX 9000

#### Syntax

`event-history-size [high|low|medium]`

#### Parameters

`event-history-size [high|low|medium]`

|                                                   |                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>event-history-size [high low medium]</code> | Defines the size of the NSight event history collection. The options are: <ul style="list-style-type: none"> <li>• high - Sets the size at approximately 10 M events</li> <li>• low - Sets the size at approximately 500 K events. This is the default setting.</li> <li>• medium - Sets the size at approximately 5 M events</li> </ul> |
|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-nsight-policy-test)#event-history-size medium
nx9500-6C8809(config-nsight-policy-test)#show context
nsight-policy test
 event-history-size medium
nx9500-6C8809(config-nsight-policy-test)#
```

## Related Commands

|                |                                                                   |
|----------------|-------------------------------------------------------------------|
| no on page 485 | Reverts the NSight event history collection size to default (5 M) |
|----------------|-------------------------------------------------------------------|

## history-ttl

Configures the TTL (time-to-live), in days, for historical data related to clients, devices, and guest users. This is the duration for which clients, devices, or guest user related data is retained in the NSight database.

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 96XX, VX 9000

## Syntax

```
history-ttl [clients|devices|guest-clients]
history-ttl [clients|devices] <1-3650>
history-ttl guest-clients <8-48>
```

## Parameters

```
history-ttl [clients|devices] <1-3650>
```

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| history-ttl [clients devices] <1-3650> | <p>Configures the TTL for historical data related to clients and devices</p> <ul style="list-style-type: none"><li>• clients - Configures the TTL for wireless clients related historical data</li><li>• devices - Configures the TTL for devices (adopted access points or site controllers) related historical data</li></ul> <p>The following is common to both the 'clients' and 'devices' keywords:</p> <ul style="list-style-type: none"><li>• &lt;1-3650&gt; - Specify a value from 1 - 3650 days. The default for both (clients and devices) is 180 days.</li></ul> |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
history-ttl guest-clients <8-48>
```

|                                  |                                                                                                                                                                                                                                                                                                |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| history-ttl guest-clients <8-48> | <p>Configures the TTL for historical data related to clients and devices</p> <ul style="list-style-type: none"><li>• guest-clients - Configures the TTL for guest-client related historical data</li><li>• &lt;8-48&gt; - Specify a value from 8 - 48 hours. The default is 8 hours.</li></ul> |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-nsight-policy-test)#history-ttl clients 250
nx9500-6C8809(config-nsight-policy-test)#show context
nsight-policy test
 history-ttl clients 250
nx9500-6C8809(config-nsight-policy-test)#
```

## Related Commands

|                |                                                                          |
|----------------|--------------------------------------------------------------------------|
| no on page 485 | Reverts the NSight clients or devices TTL duration to default (180 days) |
|----------------|--------------------------------------------------------------------------|

## mandatory

Configures mandatory AVC statistics reporting for a specified application group. When configured, the RF Domain manager reports usage stats for applications, in the specified group, to the NSight server. By default, only the top-ten applications by usage are reported to the NSight server. This option allows you to configure mandatory stats reporting for applications that are not in the top-ten list.

To enable mandatory statistics reporting for an application or set of applications, create an application group, add the desired application(s), and enable mandatory stats reporting for the group. Once enabled, the specified application(s) usage stats is always reported.

At any given time, only ten (10) applications can be reported to the NSight server. These are the top-ten applications, by usage, identified by the system. However, if mandatory application stats reporting is enabled, applications, within the specified application group, have to be included in the report. This is done by dropping some of the top-ten applications. For example, if mandatory application reporting is enabled for five (5) applications, the report will contain these 5 applications, plus first 5 of the top-ten applications identified by the system, totaling the number to ten.

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 96XX, VX 9000

#### Syntax

```
mandatory app stats app-group <APPLICATION-GROUP-NAME>
```

#### Parameters

```
mandatory app stats app-group <APPLICATION-GROUP-NAME>
```

|                                    |                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mandatory app stats                | Enables mandatory AVC statistics reporting for a specified application group                                                                                                                                                                                                                                                                                                                                             |
| app-group <APPLICATION-GROUP-NAME> | Specifies the application group for which statistics reporting is to be made mandatory. When configured, usage statistics, for the specified application group, is always reported to the NSight server. <ul style="list-style-type: none"> <li>• &lt;APPLICATION-GROUP-NAME&gt; - Specify the application group name.</li> </ul> <p><b>Note:</b> An application group can have a maximum of eight (8) applications.</p> |

#### Examples

```
nx9500-6C8809(config-nsight-policy-test)#mandatory app stats app-group socialnetworking
nx9500-6C8809(config-nsight-policy-test)#show context
nsight-policy test
server host 1.2.3.4 https
```

```
nx9500-6C8809(config-nsight-policy-test)#
```

Following is the "socialnetworking" application-group configuration. It contains three applications, which will be always reported to the NSight server even if they are not in the top-ten applications by usage list.

```
nx9500-6C8809(config-app-group-socialnetworking)#show context
application-group socialnetworking
 application facetime
 application Facebook_chat
 application "Google Hangouts_audio"
nx9500-6C8809(config-app-group-socialnetworking)#
```

#### Related Commands

|                |                                                           |
|----------------|-----------------------------------------------------------|
| no on page 485 | Disables mandatory application usage statistics reporting |
|----------------|-----------------------------------------------------------|

## nsight-server

Enables NSight server functionality and configures the SMTP report delivery settings.

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 96XX, VX 9000

### Syntax

```
nsight-server {smtp-report-delivery/standalone}
nsight-server {smtp-report-delivery host <WORD> sender <EMAIL-ADD>
[port <1-65535>|security [none|ssl|starttls]|username <USER-NAME> password [0|2|<WORD>]]}
nsight-server {standalone}
```

### Parameters

```
nsight-server {smtp-report-delivery host <WORD> sender <EMAIL-ADD>
[port <1-65535>|security [none|ssl|starttls]|username <USER-NAME> password [0|2|<WORD>]]}
```

|                                               |                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| nsight-server                                 | Enables NSight server functionality on the host using this NSight policy                                                                                                                                                                                                                                                                                              |
| smtp-report-delivery host <WORD>              | Optional. Configures SMTP report delivery settings <ul style="list-style-type: none"><li>• host &lt;WORD&gt; - Configures the SMTP server host<ul style="list-style-type: none"><li>• &lt;WORD&gt; - Specify the SMTP server host's IP address or hostname.</li></ul></li></ul>                                                                                       |
| sender <EMAIL-ADD>                            | Optional. Configures the SMTP sender's e-mail address <ul style="list-style-type: none"><li>• &lt;EMAIL-ADD&gt; - Specify the sender's e-mail address.</li></ul>                                                                                                                                                                                                      |
| port <1-65535>                                | Optional. Configures the SMTP server port <ul style="list-style-type: none"><li>• &lt;1-65535&gt; - Specify the port from 1 - 65535.</li></ul>                                                                                                                                                                                                                        |
| security [none ssl starttls]                  | Optional. Configures the encryption protocol used by the SMTP server. The options are: <ul style="list-style-type: none"><li>• none - Uses no encryption</li><li>• ssl - Uses SSL encryption</li><li>• starttls - Uses STARTTLS encryption</li></ul>                                                                                                                  |
| username <USER-NAME><br>password [0 2 <WORD>] | Optional. Configures the SMTP username <ul style="list-style-type: none"><li>• &lt;USER-NAME&gt; Specify the user name<ul style="list-style-type: none"><li>• password [0 2 &lt;WORD&gt;] - Configures the password associated with the above configured user<ul style="list-style-type: none"><li>• &lt;WORD&gt; - Enter the password.</li></ul></li></ul></li></ul> |

```
nsight-server {standalone}
```

|               |                                                                                                                                                                              |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| nsight-server | Enables NSight server functionality on the host using this NSight policy                                                                                                     |
| standalone    | Optional. Configures NSight server as standalone. Use this option in the split NSight deployment scenario where the NSight server and database are hosted on separate hosts. |

### Examples

```
nx9510-6C8A5C(config-nsight-policy-test2)#nsight-server
nx9510-6C8A5C(config-nsight-policy-test2)#show context
nsight-policy test2
 nsight-server
nx9510-6C8A5C(config-nsight-policy-test2)#
```

### Related Commands



no on page 485

Disables NSight server functionality on this NSight policy

## server

Configures the NSight server host. This configuration is used by the NSight client to identify the NSight server host.

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 96XX, VX 9000

### Syntax

```
server host [<IP>|<HOSTNAME>|<X:X::X:X>] {http|https}
```

### Parameters

```
server host [<IP>|<HOSTNAME>|<X:X::X:X>] {http|https}
```

```
server host [<IP>|
<HOSTNAME>|<X:X::X:X>]
```

Configures the NSight server host's address. Use one of the following options to identify the NSight server host:

- <IP> - Configures the NSight server's IPv4 address
- <HOSTNAME> - Configures the NSight server's hostname
- <X:X::X:X> - Configures the NSight server's IPv6 address

```
{http|https}
```

Optional. Configures the protocol used to communicate with the NSight server

- http - Optional. Uses HTTP to communicate
- https - Optional. Uses HTTPS to communicate (this is the default setting)

### Examples

```
nx9510-6C8A5C(config-nsight-policy-test2)#server host 172.22.0.153 http
nx9510-6C8A5C(config-nsight-policy-test2)#show context
nsight-policy test2
 server host 172.22.0.153 http
 nsight-server
nx9510-6C8A5C(config-nsight-policy-test2)#
```

### Related Commands

no on page 485

Removes NSight server host settings from this NSight policy

## no

Removes NSight policy settings or reverts them to default values

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 96XX, VX 9000

### Syntax

```
no [enable|event-history-size|history-ttl [clients|devices|guest-clients] |
mandatory app stats app-group <APPLICATION-GROUP-NAME> |
nsight-server {smtp-report-delivery}|server host [<IP>|<HOSTNAME>|<X:X::X:X>]]
```

### Parameters

```
no <PARAMETERS>
```

```
no <PARAMETERS>
```

Removes NSight policy settings based on the parameters passed

### Examples

The following example shows the NSight policy 'test2' settings before the 'no' command is executed:

```
nx9510-6C8A5C(config-nsight-policy-test2)#show context
nsight-policy test2
 server host 172.22.0.153 http
 nsight-server
nx9510-6C8A5C(config-nsight-policy-test2)#
nx9510-6C8A5C(config-nsight-policy-test2)#no server host 172.22.0.153
```

The following example shows the NSight policy 'test2' settings after the 'no' command is executed:

```
nx9500-6C8809(config-nsight-policy-test2)#show context
nsight-policy test2
 nsight-server
nx9510-6C8A5C(config-nsight-policy-test2)#
```

### *passpoint-policy*

Creates a new passpoint policy and enters its configuration mode

The passpoint policy implements the Hotspot 2.0 Wi-Fi Alliance standard, enabling interoperability between clients, infrastructure, and operators. It makes a portion of the IEEE 802.11u standard mandatory and adds Hotspot 2.0 extensions that allow clients to query a network before actually attempting to join it.

The passpoint policy allows a single or set of Hotspot 2.0 configurations to be global and referenced by the devices that use it. It is mapped to a WLAN. However, only primary WLANs on a BSSID will have their passpoint policy configuration used.

#### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### **Syntax**

```
passpoint-policy <POLICY-NAME>
```

#### **Parameters**

```
passpoint-policy <POLICY-NAME>
```

|                                |                                                                                                                 |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------|
| passpoint-policy <POLICY-NAME> | Specify the passpoint policy name. If a passpoint policy with the specified name does not exist, it is created. |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------|

#### **Examples**

```
nx9500-6C8809(config)#passpoint-policy test
nx9500-6C8809(config-passpoint-policy-test)#?
```

Passpoint Policy Mode commands:

|                       |                                                       |
|-----------------------|-------------------------------------------------------|
| 3gpp                  | Configure a 3gpp plmn (public land mobile network) id |
| access-network-type   | Set the access network type for the passpoint         |
| connection-capability | Configure the connection capability for the passpoint |
| domain-name           | Add a domain-name for the passpoint                   |
| hessid                | Set a homogeneous ESSID value for the passpoint       |
| internet              | Advertise the passpoint having internet access        |
| ip-address-type       | Configure the advertised ip-address-type              |
| nai-realm             | Configure a NAI realm for the passpoint               |
| net-auth-type         | Add a network authentication type to the passpoint    |

|                 |                                                            |
|-----------------|------------------------------------------------------------|
| no              | Negate a command or set its defaults                       |
| operator        | Add configuration related to the operator of the passpoint |
| osu             | Online signup                                              |
| roam-consortium | Add a roam consortium for the passpoint                    |
| venue           | Set the venue parameters of the passpoint                  |
| wan-metrics     | Set the wan-metrics of the passpoint                       |
|                 |                                                            |
| clrscr          | Clears the display screen                                  |
| commit          | Commit all changes made in this session                    |
| do              | Run commands from Exec mode                                |
| end             | End current mode and change to EXEC mode                   |
| exit            | End current mode and down to previous mode                 |
| help            | Description of the interactive help system                 |
| revert          | Revert changes                                             |
| service         | Service Commands                                           |
| show            | Show running system information                            |
| write           | Write running configuration to memory or terminal          |

```
nx9500-6C8809(config-passpoint-policy-test)#
```

### Related Commands

|                 |                                           |
|-----------------|-------------------------------------------|
| <code>no</code> | Removes an existing roam passpoint policy |
|-----------------|-------------------------------------------|



#### Note

For more information on Passpoint policy, see [PASSPOINT-POLICY](#)

### *password-encryption*

Enables password encryption and configures the passphrase used to encrypt passwords. When enabled, passwords configured within the system are not displayed as clear text.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
password-encryption secret 2 <LINE>
```

#### Parameters

```
password-encryption secret 2 <LINE>
```

|                 |                                                                                                                                                                                                                    |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| secret 2 <LINE> | Encrypts passwords with a secret phrase <ul style="list-style-type: none"> <li>• 2 - Specifies the encryption type as either SHA256-AES256</li> <li>• &lt;LINE&gt; - Specify the encryption passphrase.</li> </ul> |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config)#password-encryption secret 2 test@123
```

To confirm if password encryption is enabled, execute the following command:

```
nx9500-6C8809(config)#show password-encryption status
Password encryption is enabled
nx9500-6C8809(config)#
```

The following example shows the privilege-mode-password as encrypted text. Note, the digit '1' preceding the password implies that displayed text is the encrypted password and not clear text.

```
nx9500-6C8809(config-management-policy-test)#show context include-factory |
include privilege-mode-password
 privilege-mode-password 1 bc28e4d82bb11fa75a3c56346441d48f50f19c47184e2575a59a6a5d18e63925
nx9500-6C8809(config-management-policy-test)#
```

## Related Commands

|    |                              |
|----|------------------------------|
| no | Disables password encryption |
|----|------------------------------|

## profile

Configures profile related commands. If no parameters are given, all profiles are selected.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
profile {anyap/ap6522/ap6562/ap71xx/ap7502/ap7522/ap7532/ap7562/ap7602/ap7612/ap7622/
ap7632/ap7662/ap81xx/ap8432/ap8533/containing/filter/rfs4000/nx5500/nx75xx/nx9000/
nx9600/vx9000}
profile {anyap/ap6522/ap6562/ap71xx/ap7502/ap7522/ap7532/ap7562/ap7602/ap7612/ap7622/
ap7632/ap7662/ap81xx/ap8432/ap8533/rfs4000/nx5500/nx75xx/nx9000/nx9600/vx9000}
<DEVICE-PROFILE-NAME>
profile {containing <DEVICE-PROFILE-NAME>} {filter type [ap6522/ap6562/ap71xx/
ap7502/ap7522/ap7532/ap7602/ap7612/ap7622/ap7632/ap7662/ap81xx/ap8432/ap8533/rfs4000/
nx75xx/nx9000/vx9000]}
profile {filter type [ap6522/ap6562/ap71xx/ap7502/ap7522/ap7532/ap7562/ap7602/
ap7612/ap7622/ap7632/ap7662/ap81xx/ap8432/ap8533/rfs4000/rfs6000/nx5500/nx75xx/nx9000/
nx9600/vx9000]}
```

### Parameters

```
profile {anyap/ap6522/ap6562/ap71xx/ap7502/ap7522/ap7532/ap7562/ap7602/ap7612/ap7622/
ap7632/ap7662/ap81xx/ap8432/ap8533/rfs4000/rfs6000/nx5500/nx75xx/nx9000/nx9600/vx9000}
<DEVICE-PROFILE-NAME>
```

|                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| profile<br><DEVICE-<br>TYPE><br><DEVICE-<br>PROFILE-<br>NAME> | <p>Configures device profile commands. If no device profile is specified, the system configures all device profiles.</p> <ul style="list-style-type: none"> <li>&lt;DEVICE-TYPE&gt; - Optional. Select the device type. The options are: AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533 RFS 4000, NX 5500, NX 7510, NX 95XX, NX 96XX, and VX 9000.</li> </ul> <p>After specifying the device type, specify the profile name.</p> <ul style="list-style-type: none"> <li>&lt;DEVICE-PROFILE-NAME&gt; - Specify the profile name.</li> </ul> <p>Select 'anyap' to configure a profile applicable to any access point.</p> |
|---------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
profile {containing <DEVICE-PROFILE-NAME>} {filter type [ap6522/ap6562/ap71xx/
ap7502/ap7522/ap7532/ap7562/ap7602/ap7612/ap7622/ap7632/ap7662/ap81xx/ap8432/ap8533/
rfs4000/nx5500/nx75xx/nx9000/nx9600/vx9000]}
```

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| profile                                     | Configures device profile commands                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| containing<br><DEVICE-<br>PROFILE-<br>NAME> | <p>Optional. Configures profiles that contain a specified sub-string in the hostname</p> <ul style="list-style-type: none"> <li>&lt;DEVICE-PROFILE-NAME&gt; - Specify a substring in the profile name to filter profiles.</li> </ul>                                                                                                                                                                                                                                                                                 |
| filter type                                 | <p>Optional. An additional filter used to configure a specific type of device profile. If no device type is specified, the system configures all device profiles.</p> <ul style="list-style-type: none"> <li>type - Filters profiles by the device type. Select a device type from the following options: AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533 RFS 4000, NX 5500, NX 7510, NX 95XX, NX 96XX, and VX 9000</li> </ul> |

```
profile {filter type[ap6522/ap6562/ap71xx/ap7502/ap7522/ap7532/ap7562/ap7602/
ap7612/ap7622/ap7632/ap7662/ap81xx/ap8432/ap8533/rfs4000/rfs6000/nx5500/nx75xx/nx9000/
nx9600/vx9000]}
```

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| profile     | Configures device profile commands                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| filter type | <p>Optional. An additional filter used to configure a specific type of device profile. If no device type is specified, the system configures all device profiles.</p> <ul style="list-style-type: none"> <li>type - Filters profiles by the device type. Select a device type from the following options: AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533 RFS 4000, NX 5500, NX 7510, NX 95XX, NX 96XX, and VX 9000</li> </ul> |

## Examples

```
<DEVICE>(config)#profile nx9000 test-NX9500
```

```
<DEVICE>(config-profile-test-NX9500)#?
```

```
Profile Mode commands:
```

|                                         |                                                                             |
|-----------------------------------------|-----------------------------------------------------------------------------|
| adopter-auto-provisioning-policy-lookup | Use centralized auto-provisioning policy when adopted by another controller |
| adoption                                | Adoption configuration                                                      |
| adoption-mode                           | Configure the adoption mode for the access-points in this RF-Domain         |
| alias                                   | Alias                                                                       |
| application-policy                      | Application Policy configuration                                            |
| area                                    | Set name of area where the system is located                                |
| arp                                     | Address Resolution Protocol (ARP)                                           |
| auto-learn                              | Auto learning                                                               |

|                                    |                                                                                 |
|------------------------------------|---------------------------------------------------------------------------------|
| autogen-uniqueid                   | Autogenerate a unique id                                                        |
| autoinstall                        | Autoinstall settings                                                            |
| bridge                             | Ethernet bridge                                                                 |
| captive-portal                     | Captive portal                                                                  |
| cdp                                | Cisco Discovery Protocol                                                        |
| cluster                            | Cluster configuration                                                           |
| configuration-persistence          | Enable persistence of configuration across reloads (startup config file)        |
| controller                         | WLAN controller configuration                                                   |
| critical-resource                  | Critical Resource                                                               |
| crypto                             | Encryption related commands                                                     |
| database                           | Database command                                                                |
| device-onboard                     | Device-onboarding configuration                                                 |
| device-upgrade                     | Device firmware upgrade                                                         |
| diag                               | Diagnosis of packets                                                            |
| dot1x                              | 802.1X                                                                          |
| dpi                                | Enable Deep-Packet-Inspection (Application Assurance)                           |
| dscp-mapping                       | Configure IP DSCP to 802.1p priority mapping for untagged frames                |
| eguest-server                      | Enable ExtremeGuest Server functionality                                        |
| email-notification                 | Email notification configuration                                                |
| enforce-version                    | Check the firmware versions of devices before interoperating                    |
| environmental-sensor               | Environmental Sensors Configuration                                             |
| events                             | System event messages                                                           |
| export                             | Export a file                                                                   |
| file-sync                          | File sync between controller and adoptees                                       |
| floor                              | Set the floor within a area where the system is located                         |
| gre                                | GRE protocol                                                                    |
| http-analyze                       | Specify HTTP-Analysis configuration                                             |
| interface                          | Select an interface to configure                                                |
| ip                                 | Internet Protocol (IP)                                                          |
| ipv6                               | Internet Protocol version 6 (IPv6)                                              |
| l2tpv3                             | L2tpv3 protocol                                                                 |
| l3e-lite-table                     | L3e lite Table                                                                  |
| led                                | Turn LEDs on/off on the device                                                  |
| led-timeout                        | Configure the time for the led to turn off after the last radio state change    |
| legacy-auto-downgrade              | Enable device firmware to auto downgrade when other legacy devices are detected |
| legacy-auto-update                 | Auto upgrade of legacy devices                                                  |
| lldp                               | Link Layer Discovery Protocol                                                   |
| load-balancing                     | Configure load balancing parameter                                              |
| logging                            | Modify message logging facilities                                               |
| mac-address-table                  | MAC Address Table                                                               |
| mac-auth                           | 802.1X                                                                          |
| management-server                  | Configure management server address                                             |
| memory-profile                     | Memory profile to be used on the device                                         |
| meshpoint-device                   | Configure meshpoint device parameters                                           |
| meshpoint-monitor-interval         | Configure meshpoint monitoring interval                                         |
| min-misconfiguration-recovery-time | Time interval to check controller connectivity after configuration is received  |

|                                |                                                                                     |
|--------------------------------|-------------------------------------------------------------------------------------|
| mint                           | MiNT protocol                                                                       |
| misconfiguration-recovery-time | Check controller connectivity after configuration is received                       |
| neighbor-inactivity-timeout    | Configure neighbor inactivity timeout                                               |
| neighbor-info-interval         | Configure neighbor information exchange interval                                    |
| no                             | Negate a command or set its defaults                                                |
| noc                            | Configure the noc related setting                                                   |
| nsight                         | NSight                                                                              |
| ntp                            | Ntp server WORD                                                                     |
| offline-duration               | Set duration for which a device remains unadopted before it generates offline event |
| otls                           | Omnitrail Location Server                                                           |
| power-config                   | Configure power mode                                                                |
| preferred-controller-group     | Controller group this system will prefer for adoption                               |
| preferred-tunnel-controller    | Tunnel Controller Name this system will prefer for tunneling extended vlan traffic  |
| radius                         | Configure device-level radius authentication parameters                             |
| raid                           | RAID                                                                                |
| remote-debug                   | Configure remote debug parameters                                                   |
| remove-override                | Remove configuration item override from the device (so profile value takes effect)  |
| rf-domain-manager              | RF Domain Manager                                                                   |
| router                         | Dynamic routing                                                                     |
| slot                           | PCI expansion Slot                                                                  |
| spanning-tree                  | Spanning tree                                                                       |
| traffic-class-mapping          | Configure IPv6 traffic class to 802.1p priority mapping for untagged frames         |
| traffic-shape                  | Traffic shaping                                                                     |
| trustpoint                     | Assign a trustpoint to a service                                                    |
| tunnel-controller              | Tunnel Controller group this controller belongs to                                  |
| use                            | Set setting to use                                                                  |
| vrrp                           | VRRP configuration                                                                  |
| vrrp-state-check               | Publish interface via OSPF/BGP only if the interface VRRP state is not BACKUP       |
| wep-shared-key-auth            | Enable support for 802.11 WEP shared key authentication                             |
| zone                           | Configure Zone name                                                                 |
| clrscr                         | Clears the display screen                                                           |
| commit                         | Commit all changes made in this session                                             |
| do                             | Run commands from Exec mode                                                         |
| end                            | End current mode and change to EXEC mode                                            |
| exit                           | End current mode and down to previous mode                                          |
| help                           | Description of the interactive help system                                          |
| revert                         | Revert changes                                                                      |
| service                        | Service Commands                                                                    |
| show                           | Show running system information                                                     |
| write                          | Write running configuration to memory or terminal                                   |

```
<DEVICE>(config-profile-test-NX9500)#
```

## Related Commands

|                 |                                                     |
|-----------------|-----------------------------------------------------|
| <code>no</code> | Removes a profile and its associated configurations |
|-----------------|-----------------------------------------------------|



### Note

For more information on profiles and how to configure profiles, see [PROFILES](#) on page 857.

## *radio-qos-policy*

Configures a radio QoS policy

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
radio-qos-policy <RADIO-QOS-POLICY-NAME>
```

### Parameters

```
radio-qos-policy <RADIO-QOS-POLICY-NAME>
```

|                                            |                                                                                                       |
|--------------------------------------------|-------------------------------------------------------------------------------------------------------|
| <code>&lt;RADIO-QOS-POLICY-NAME&gt;</code> | Specify the radio QoS policy name. If a policy with the specified name does not exist, it is created. |
|--------------------------------------------|-------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config)#radio-qos-policy test
nx9500-6C8809(config-radio-qos-test)#?
Radio QoS Mode commands:
 accelerated-multicast Configure multicast streams for acceleration
 admission-control Configure admission-control on this radio for one or
 more access categories
 no Negate a command or set its defaults
 smart-aggregation Configure smart aggregation parameters
 wmm Configure 802.11e/Wireless MultiMedia parameters

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-radio-qos-test)#
<exsw1>(config-radio-qos-test)#
```



## Related Commands

|                 |                                      |
|-----------------|--------------------------------------|
| <code>no</code> | Removes an existing Radio QoS policy |
|-----------------|--------------------------------------|



### Note

For more information on radio qos policy, see [RADIO-QOS-POLICY](#).

## *radius-group*

Configures RADIUS user group and enters its configuration mode

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
radius-group <RADIUS-GROUP-NAME>
```

### Parameters

```
radius-group <RADIUS-GROUP-NAME>
```

|                     |                                                                                                                                                           |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <RADIUS-GROUP-NAME> | Specify a RADIUS user group name. The name should not exceed 64 characters. If a RADIUS user group with the specified name does not exist, it is created. |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config)#radius-group testRadiusGr
nx9500-6C8809(config-radius-group-testRadiusGr)#?
Radius user group configuration commands:
 guest Make this group a Guest group
 no Negate a command or set its defaults
 policy Radius group access policy configuration
 rate-limit Set rate limit for group

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-radius-group-testRadiusGr)#
```

## Related Commands

|                 |                                  |
|-----------------|----------------------------------|
| <code>no</code> | Removes an existing RADIUS group |
|-----------------|----------------------------------|



### Note

For more information on RADIUS user group commands, see [RADIUS-POLICY](#).

## *radius-server-policy*

Creates an onboard device RADIUS server policy and enters its configuration mode

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
radius-server-policy <RADIUS-SERVER-POLICY-NAME>
```

### Parameters

```
radius-server-policy <RADIUS-SERVER-POLICY-NAME>
```

|                             |                                                                                                           |
|-----------------------------|-----------------------------------------------------------------------------------------------------------|
| <RADIUS-SERVER-POLICY-NAME> | Specify the RADIUS server policy name. If a policy with the specified name does not exist, it is created. |
|-----------------------------|-----------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config)#radius-server-policy testRadiusServerPolicy
nx9500-6C8809(config-radius-server-policy-testRadiusServerPolicy)#?
Radius Configuration commands:
 authentication Radius authentication
 bypass Bypass Certificate Revocation List(CRL) check
 chase-referral Enable chasing referrals from LDAP server
 crl-check Enable Certificate Revocation List(CRL) check
 ldap-agent LDAP Agent configuration parameters
 ldap-group-verification Enable LDAP Group Verification setting
 ldap-server LDAP server parameters
 local RADIUS local realm
 nas RADIUS client
 no Negate a command or set its defaults
 proxy RADIUS proxy server
 session-resumption Enable session resumption/fast reauthentication by
 using cached attributes
 termination Enable Eap termination for proxy requests
 use Set setting to use

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
```

```
write Write running configuration to memory or terminal
nx9500-6C8809(config-radius-server-policy-testRadiusServerPolicy)#
```

### Related Commands

|    |                                          |
|----|------------------------------------------|
| no | Removes an existing RADIUS server policy |
|----|------------------------------------------|



#### Note

For more information on RADIUS server policy commands, see [RADIUS-POLICY](#).

### *radius-user-pool-policy*

Configures a RADIUS user pool policy and enters its configuration mode

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
radius-user-pool-policy <RADIUS-USER-POOL-NAME>
```

#### Parameters

```
radius-user-pool-policy <RADIUS-USER-POOL-NAME>
```

|                                |                                                                                                              |
|--------------------------------|--------------------------------------------------------------------------------------------------------------|
| <RADIUS-USER-POOL-POLICY-NAME> | Specify the RADIUS user pool policy name. If a policy with the specified name does not exist, it is created. |
|--------------------------------|--------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config)#radius-user-pool-policy testRadiusUserPool
nx9500-6C8809(config-radius-user-pool-testRadiusUserPool)#?
Radius User Pool Mode commands:
 duration Set a guest user's access duration
 no Negate a command or set its defaults
 user Radius user configuration

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-radius-user-pool-testRadiusUserPool)#
```

## Related Commands

`no` Removes an existing RADIUS user pool policy



### Note

For more information on RADIUS user group commands, see [RADIUS-POLICY](#).

## rename

Renames and existing TLO

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
rename tlo <TLO-NAME> <NEW-TLO-NAME>
```

### Parameters

```
rename tlo <TLO-NAME> <NEW-TLO-NAME>
```

|                                      |                                                                                                                                                                                                         |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| rename tlo <TLO-NAME> <NEW-TLO-NAME> | Renames an existing TLO object                                                                                                                                                                          |
|                                      | <ul style="list-style-type: none"><li>• &lt;TLO-NAME&gt; - Specify the TLO's name. This is the TLO that is to be renamed.</li><li>• &lt;NEW-TLO-NAME&gt; - Specify the new name for this TLO.</li></ul> |

### Examples

The following example shows the top level objects available for renaming:



### Note

Enter rename and press **Tab** to list top level objects available for renaming.

```
nx9500-6C8809(config)#rename [TAB]
aaa_policy aaa_tacacs_policy
address_range_alias aif_policy
app_policy application
assoc_acl auto_provisioning_policy
bgp_as_path_list bgp_community_list
bgp_extcommunity_list bgp_ip_access_list
bgp_ip_prefix_list bonjour_gw_discovery_policy
bonjour_gw_forwarding_policy bonjour_gw_query_forwarding_policy
bridging_policy captive_portal
centro_policy client_identity
client_identity_group content_cache_policy
content_filter_policy crypto_cmp_policy
database_client_policy database_policy
device_categorization dhcp_server_policy
dhcpv6_server_policy dns_whitelist
dr_route_map encrypted_string_alias
event_system_policy ex3500_ext_ip_acl
ex3500_management_policy ex3500_qos_class_map_policy
```

```

ex3500_qos_policy_map ex3500_std_ip_acl
ex3500_time_range firewall_policy
global_assoc_list guest_management
hashed_string_alias host_alias
ip_acl ip_snmp_acl
--More--
nx9500-6C8809(config)#

```

The following examples first clones the existing IP access list BROADCAST-MULTICAST-CONTROL, and then renames the cloned IP access list:

```

nx9500-6C8809(config)#show context include-factory | include ip access-list
ip access-list BROADCAST-MULTICAST-CONTROL
nx9500-6C8809(config)#
nx9500-6C8809(config)#clone ip_acl BROADCAST-MULTICAST-CONTROL Test_IP_CLONED
nx9500-6C8809(config)#commit
nx9500-6C8809(config)#show context include-factory | include ip access-list
ip access-list BROADCAST-MULTICAST-CONTROL
ip access-list Test_IP_CLONED
nx9500-6C8809(config)#
nx9500-6C8809(config)#rename Test_IP_CLONED NEW_IP_CLONED
nx9500-6C8809(config)#commit
nx9500-6C8809(config)#show context include-factory | include ip access-list
ip access-list BROADCAST-MULTICAST-CONTROL
ip access-list NEW_IP_CLONED
nx9500-6C8809(config)#

```

## Related Commands

|              |                                                |
|--------------|------------------------------------------------|
| <b>clone</b> | Creates a replica of an existing TLO or device |
|--------------|------------------------------------------------|

## replace

Selects an existing device by its MAC address or hostname and replaces it with a new device having a different MAC address. Internally, a new device is created with the new MAC address. The old device's configuration is copied to the new device, and then removed from the controller's configuration (i.e., the old device's configuration is no longer staged on the controller).

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
replace device [<MAC-ADDRESS>|<HOSTNAME>] <NEW-MAC-ADDRESS>
```

### Parameters

```
replace device [<MAC-ADDRESS>|<HOSTNAME>] <NEW-MAC-ADDRESS>
```

|                                |                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| replace-device                 | Replaces an existing device with a new device, such that the old device's configuration is copied on to the new device                                                                                                                                                                                                                                   |
| [<MAC-ADDRESS>]<br><HOSTNAME>] | Identifies the device to replace by its MAC address or hostname <ul style="list-style-type: none"> <li>• &lt;MAC-ADDRESS&gt; - Identifies the device to replace by its MAC address. Specify the device's existing MAC address.</li> <li>• &lt;HOSTNAME&gt; - Identifies the device to replace by its hostname. Specify the device's hostname.</li> </ul> |
| <NEW-MAC-ADDRESS>              | Specifies the new device's MAC address. Both the new and old devices should of the same model type.                                                                                                                                                                                                                                                      |

## Examples

```
rfs4000-882A17(config)#replace device ap7131-4BF364 ?
 AA-BB-CC-DD-EE-FF New device MAC address
rfs4000-882A17(config)#replace device ap7131-4BF364 00-15-0F-BB-98-30
```

The following example shows an existing AP7502 (MAC: DD-AA-BB-88-12-43) configuration staged on a VX9000 controller:

```
VX9000-NOC-DE9D(config-device-DD-AA-BB-88-12-43)#show context
ap7502 DD-AA-BB-88-12-43
 use profile default-ap7502
 use rf-domain default
 hostname ap7502-881243
 interface radiol
 wlan theMOZART bss 1 primary
 interface radio2
 wlan theMOZART bss 1 primary
 interface gel
 switchport mode access
 switchport access vlan 1
 controller host 12.12.12.2
VX9000-NOC-DE9D(config-device-DD-AA-BB-88-12-43)#
```

The following example shows AP7502 (MAC: DD-AA-BB-88-12-43) replaced by another AP7502 having MAC address 11-22-33-44-55-66:

Note that the new AP7502 device has the same configuration as the old AP7502 device. The HOSTNAME remains the same. Consequently, objects that refer to this particular hostname need not be updated. For example, an hostname alias identifying this particular device, and TLOs using this alias, such as IP/MAC ACLs, remain unchanged.

```
VX9000-NOC-DE9D(config)#replace device DD-AA-BB-88-12-43 11-22-33-44-55-66
VX9000-NOC-DE9D(config)#ap7502 11-22-33-44-55-66
VX9000-NOC-DE9D(config-device-11-22-33-44-55-66)#show context
ap7502 11-22-33-44-55-66
 use profile default-ap7502
 use rf-domain default
 hostname ap7502-881243
 interface radiol
 wlan theMOZART bss 1 primary
 interface radio2
 wlan theMOZART bss 1 primary
 interface gel
 switchport mode access
 switchport access vlan 1
 controller host 12.12.12.2
VX9000-NOC-DE9D(config-device-11-22-33-44-55-66)#
```

---

## *rf-domain*

Creates an RF Domain or enters the RF Domain configuration context for one or more RF Domains.

The configuration of controllers (wireless controllers, service platforms, and access points) comprises of RF Domains that define regulatory, location, and other relevant policies. At least one default RF Domain is assigned to each controller. RF Domains allow administrators to assign configuration data to multiple devices deployed in a common coverage area, such as in a floor, building, or site. Each RF Domain contains policies that set the Smart RF or WIPS configuration.

RF Domains also enable administrators to override WLAN SSID name and VLAN assignments. This enables the deployment of a global WLAN across multiple sites and unique SSID name or VLAN assignments to groups of access points servicing the global WLAN. This WLAN override eliminates the need to define and manage a large number of individual WLANs and profiles.

A controller's configuration contains:

- A default RF Domain - Each controller utilizes a default RF Domain. Access Points are assigned to this default RF Domain as they are discovered by the controller. A default RF Domain can be used for single-site and multi-site deployments.
- Single-site deployment - The default RF Domain can be used for single site deployments, where regional, regulatory, and RF policies are common between devices.
- Multi-site deployment - A default RF Domain can omit configuration parameters to prohibit regulatory configuration from automatically being inherited by devices as they are discovered. This is desirable in multi-site deployments with devices spanning multiple countries. Omitting specific configuration parameters eliminates the risk of an incorrect country code from being automatically assigned to a device.
- A user-defined RF Domain - Created by administrators. A user-defined RF Domain can be assigned to multiple devices manually or automatically.
- Manually assigned - Use the CLI or UI to manually assign a user-defined RF Domain to controllers and service platforms.
- Automatically assigned - Use a AP provisioning policy to automatically assign specific RF Domains to access points based on the access point's model, serial number, VLAN, DHCP option, and IP address or MAC address. Automatic RF Domain assignments are useful in large deployments, as they enable plug-n-play access point deployments by automatically applying RF Domains to remote access points. For more information on auto provisioning policy, see [AUTO-PROVISIONING-POLICY](#).

Configure and deploy user-defined RF Domains for single or multiple sites where devices require unique regulatory and regional configurations, or unique Smart RF and WIPS policies. User-defined RF Domains can be used to:

- Assign unique Smart RF or WIPS policies to access points deployed on different floors or buildings within in a site.
- Assign unique regional or regulatory configurations to devices deployed in different states or countries.
- Assign unique WLAN SSIDs and/or VLAN IDs to sites assigned a common WLAN without having to define individual WLANs for each site.

### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533

- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
rf-domain {<RF-DOMAIN-NAME>/containing <RF-DOMAIN-NAME>}
```

## Parameters

```
rf-domain {<RF-DOMAIN-NAME>/containing <RF-DOMAIN-NAME>}
```

|                             |                                                                                                                                                                                                                             |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| rf-domain                   | Creates a new RF Domain or enters its configuration context                                                                                                                                                                 |
| <RF-DOMAIN-NAME>            | Optional. Specify the RF Domain name (should not exceed 32 characters and should represent the intended purpose). Once created, the name cannot be edited.                                                                  |
| containing <RF-DOMAIN-NAME> | Optional. Identifies an existing RF Domain that contains a specified sub-string in the domain name <ul style="list-style-type: none"> <li>• &lt;RF-DOMAIN-NAME&gt; - Specify a sub-string of the RF Domain name.</li> </ul> |

## Examples

```
nx9500-6C8809(config)#rf-domain ecospace
nx9500-6C8809(config-rf-domain-ecospace)#?
RF Domain Mode commands:
 alias Alias
 channel-list Configure channel list to be advertised to wireless
 clients
 contact Configure the contact
 control-vlan VLAN for control traffic on this RF Domain
 controller-managed RF Domain manager for this domain will be an adopting
 controller
 country-code Configure the country of operation
 geo-coordinates Configure geo coordinates for this device
 layout Configure layout
 location Configure the location
 location-server Configuration ExtremeLocation server
 location-tenantid Set ExtremeLocation tenant id
 mac-name Configure MAC address to name mappings
 no Negate a command or set its defaults
 nsight-sensor Enable sensor for Nsight
 override-smarttrf Configured RF Domain level overrides for smart-rf
 override-wlan Configure RF Domain level overrides for wlan
 sensor-server AirDefense sensor server configuration
 stats Configure the stats related setting
 timezone Configure the timezone
 tree-node Configure tree node under which this rf-domain appears
 use Set setting to use

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-rf-domain-ecospace)#
```



## Related Commands

| Command         | Description                                                  |
|-----------------|--------------------------------------------------------------|
| <code>no</code> | Removes an existing RF Domain. Specify the RF Domain's name. |

## rf-domain-mode-commands

The following table lists the RF Domain configuration mode commands:

Table: RF-Domain Config Mode Commands

| Command                                    | Description                                                                                                                                            |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>alias</code>                         | Creates various types of aliases, such as network, VLAN, network-group, network-service, encrypted-string, hashed -string, etc. at the RF Domain level |
| <code>channel-list</code>                  | Configures the channel list advertised by radios                                                                                                       |
| <code>contact</code>                       | Configures network administrator's contact information (needed in case of any problems impacting the RF Domain)                                        |
| <code>control-vlan</code>                  | Configures VLAN for traffic control on a RF Domain                                                                                                     |
| <code>controller-managed</code>            | Configures the adopting controller or service platform as this RF Domain's manager                                                                     |
| <code>country-code</code>                  | Configures the country of operation                                                                                                                    |
| <code>geo-coordinates</code> on page 513   | Configures the longitude and latitude of the RF Domain in order to fix its exact geographical location on a map                                        |
| <code>layout</code>                        | Configures layout information                                                                                                                          |
| <code>location</code>                      | Configures the physical location of an RF Domain                                                                                                       |
| <code>location-server</code> on page 515   | Configures an ExtremeLocation server on the selected RF Domain. This command is supported only on the NX 95XX series service platforms.                |
| <code>location-tenantid</code> on page 516 | Configures the ExtremeLocation Tenant's account number                                                                                                 |
| <code>mac-name</code>                      | Maps MAC addresses to names                                                                                                                            |
| <code>no</code>                            | Negates a command or reverts configured settings to their default                                                                                      |
| <code>override-smart-rf</code>             | Configures RF Domain level overrides for Smart RF                                                                                                      |
| <code>override-wlan</code>                 | Configures RF Domain level overrides for a WLAN                                                                                                        |
| <code>sensor-server</code>                 | Configures an AirDefense sensor server on this RF Domain                                                                                               |
| <code>stats</code>                         | Configures stats related settings on this RF Domain. These settings define how RF Domain statistics are updated.                                       |
| <code>timezone</code>                      | Configures a RF Domain's geographic time zone                                                                                                          |
| <code>tree-node</code>                     | Configures the hierarchical (tree-node) structure under which this RF Domain appears                                                                   |
| <code>use</code>                           | Enables the use of a specified Smart RF and/or WIPS policy with this RF Domain                                                                         |

alias

Configures network, VLAN, host, string, network-service, etc. aliases at the RF Domain level

For information on aliases, see [alias](#).

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
alias [address-range|encrypted-string|hashed-string|host|network|network-group|
network-service|number|string|vlan]
alias encrypted-string <ENCRYPTED-STRING-ALIAS-NAME> [0|2] <LINE>
alias hashed-string <HASHED-STRING-ALIAS-NAME> 1 <LINE>
alias address-range <ADDRESS-RANGE-ALIAS-NAME> <STARTING-IP> to <ENDING-IP>
alias host <HOST-ALIAS-NAME> <HOST-IP>
alias network <NETWORK-ALIAS-NAME> <NETWORK-ADDRESS/MASK>
alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range|host|network]
alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range <STARTING-IP> to
<ENDING-IP> {<STARTING-IP> to <ENDING-IP>}|host <HOST-IP> {<HOST-IP>}|
network <NETWORK-ADDRESS/MASK> {<NETWORK-ADDRESS/MASK>}]
alias network-service <NETWORK-SERVICE-ALIAS-NAME> proto [<0-254>|<WORD>|eigrp|
gre|igmp|igmp|ospf|vrrp] {(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|
ldap|nntp|ntp|pop3|proto|sip|smtp|sourceport [<1-65535>|<WORD>]|ssh|telnet|tftp|www)}
alias number <NUMBER-ALIAS-NAME> <0-4294967295>
alias network-service <NETWORK-SERVICE-ALIAS-NAME> proto [<0-254>|<WORD>|eigrp|gre|
igmp|igmp|ospf|vrrp] {(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|
ntp|pop3|proto|sip|smtp|sourceport [<1-65535>|<WORD>]|ssh|telnet|tftp|www)}
alias string <STRING-ALIAS-NAME> <LINE>
alias vlan <VLAN-ALIAS-NAME> <1-4094>
```

### Parameters

```
alias address-range <ADDRESS-RANGE-ALIAS-NAME> <STARTING-IP> to <ENDING-IP>
```

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| address-range<br><ADDRESS-RANGE-ALIAS-NAME> | Creates a new address-range alias for this RF Domain. Or associates an existing address-range alias with this RF Domain. An address-range alias maps a name to a range of IP addresses. <ul style="list-style-type: none"><li>• &lt;ADDRESS-RANGE-ALIAS-NAME&gt; - Specify the address range alias name.</li></ul> <p><b>Note:</b> Alias name should begin with '\$'.</p>                                                                                                                                                   |
| <STARTING-IP> to<br><ENDING-IP>             | Associates a range of IP addresses with this address range alias <ul style="list-style-type: none"><li>• &lt;STARTING-IP&gt; - Specify the first IP address in the range.</li><li>• to &lt;ENDING-IP&gt; - Specify the last IP address in the range.</li></ul> <p><b>Note:</b> Aliases defined at any given level can be overridden at the next lower level. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence.</p> |

```
alias encrypted-string <ENCRYPTED-STRING-ALIAS-NAME> [0|2] <LINE>
```

|                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>encrypted-string &lt;ENCRYPTED-STRING-ALIAS-NAME&gt;</pre> | <p>Creates an alias for an encrypted string. Use this alias for string configuration values that are encrypted when "password-encryption" is enabled. For example, in the management-policy, use it to define the SNMP community string. For more information, see <a href="#">snmp-server</a>.</p> <ul style="list-style-type: none"> <li>• &lt;ENCRYPTED-STRING-ALIAS-NAME&gt; - Specify the encrypted-string alias name.</li> </ul> <p><b>Note:</b> Alias name should begin with '\$'.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <pre>[0/2] &lt;LINE&gt;</pre>                                   | <p>Configures the value associated with the alias name specified in the previous step</p> <ul style="list-style-type: none"> <li>• [0/2] &lt;LINE&gt; - Configures the alias value</li> </ul> <p>Note, if password-encryption is enabled, in the <b>show &gt; running-config</b> output, this clear text is displayed as an encrypted string, as shown below:</p> <pre>nx9500-6C8809(config)#show running-config !..... alias encrypted-string \$enString 2 fABMK2is7UToNiZE3MQXbgAAA AxBOZIysdqsEJwr6AH/Da// ! --More-- nx9500-6C8809</pre> <p>In the above output, the '2' displayed before the encrypted-string alias value indicates that the displayed text is encrypted and not a clear text. However, if password-encryption is disabled the clear text is displayed as is:</p> <pre>nx9500-6C8809(config)#show running-config !..... alias encrypted-string \$enString 0 test11223344 ! --More-- nx9500-6C8809</pre> <p>For more information on enabling password-encryption, see <a href="#">password-encryption</a>.</p> |

```
alias hashed-string <HASHED-STRING-ALIAS-NAME> <LINE>
```

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| hashed-string <HASHED-STRING-ALIAS-NAME> | <p>Creates an alias for a hashed string. Use this alias for configuration values that are hashed string, such as passwords. For example, in the management-policy, use it to define the privilege mode password. For more information, see privilege-mode-password.</p> <ul style="list-style-type: none"> <li>• &lt;HASHED-STRING-ALIAS-NAME&gt; – Specify the hashed-string alias name.</li> </ul> <p><b>Note:</b> Alias name should begin with '\$'.</p>                                                                      |
| <LINE>                                   | <p>Configures the hashed-string value associated with this alias.</p> <pre>nx9500-6C8809(config)#show running-config ! alias encrypted-string \$WRITE 2 sBqVCDaOxs3oByF5PCSuFAAA AAAd7HT2+EtT/1/BXm9c4SBDv ! alias hashed-string \$PriMode 1 faffdde27cb49ad634ea20df4f 7c8ef2685894d10ffcb1b2efba054112ecfc75 --More-- nx9500-6C8809</pre> <p>In the above <b>show &gt; running-config</b> output, the '!' displayed before the hashed-string alias value indicates that the displayed text is hashed and not a clear text.</p> |

**alias host** <HOST-ALIAS-NAME> <HOST-IP>

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| host <HOST-ALIAS-NAME> | <p>Creates a host alias for this RF Domain. Or associates an existing host alias with this RF Domain. A host alias maps a name to a single network host.</p> <ul style="list-style-type: none"> <li>• &lt;HOST-ALIAS-NAME&gt; – Specify the host alias name.</li> </ul> <p><b>Note:</b> Alias name should begin with '\$'.</p>                                                                                                                  |
| <HOST-IP>              | <p>Associates the network host's IP address with this host alias</p> <ul style="list-style-type: none"> <li>• &lt;HOST-IP&gt; – Specify the network host's IP address.</li> </ul> <p><b>Note:</b> Aliases defined at any given level can be overridden at the next lower levels. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence.</p> |

**alias network** <NETWORK-ALIAS-NAME> <NETWORK-ADDRESS/MASK>

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| network <NETWORK-ALIAS-NAME> | <p>Creates a network alias for this RF Domain. Or associates an existing network alias with this RF Domain. A network alias maps a name to a single network address.</p> <ul style="list-style-type: none"> <li>• &lt;NETWORK-ALIAS-NAME&gt; – Specify the network alias name.</li> </ul> <p><b>Note:</b> Alias name should begin with '\$'.</p>                                                                                                    |
| <NETWORK-ADDRESS/MASK>       | <p>Associates a single network with this network alias</p> <ul style="list-style-type: none"> <li>• &lt;NETWORK-ADDRESS/MASK&gt; – Specify the network's address and mask.</li> </ul> <p><b>Note:</b> Aliases defined at any given level can be overridden at the next lower levels. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence.</p> |

**alias network-group** <NETWORK-GROUP-ALIAS-NAME> [address-range <STARTING-IP> to <ENDING-IP> {<STARTING-IP> to <ENDING-IP>}|host <HOST-IP> {<HOST-IP>}|network <NETWORK-ADDRESS/MASK> {<NETWORK-ADDRESS/MASK>}]

|                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| network <NETWORK-GROUP-ALIAS-NAME>                                                    | <p>Creates a network-group alias for this RF Domain. Or associates an existing network-group alias with this RF Domain.</p> <ul style="list-style-type: none"> <li>• &lt;NETWORK-GROUP-ALIAS-NAME&gt; – Specify the network-group alias name.</li> </ul> <p><b>Note:</b> Alias name should begin with '\$'.</p> <p>After specifying the name, specify the following: a range of IP addresses, host addresses, or a range of network addresses.</p> <p><b>Note:</b> Aliases defined at any given level can be overridden at the next lower levels. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence.</p> |
| address-range<br><STARTING-IP> to<br><ENDING-IP><br>{<STARTING-IP> to<br><ENDING-IP>} | <p>Associates a range of IP addresses with this network-group alias</p> <ul style="list-style-type: none"> <li>• &lt;STARTING-IP&gt; – Specify the first IP address in the range.</li> <li>• to &lt;ENDING-IP&gt; – Specify the last IP address in the range.</li> <li>• &lt;STARTING-IP&gt; to &lt;ENDING-IP&gt; – Optional. Specifies more than one range of IP addresses. A maximum of eight (8) IP address ranges can be configured.</li> </ul>                                                                                                                                                                                                                                                              |
| host <HOST-IP> {<HOST-IP>}                                                            | <p>Associates a single or multiple hosts with this network-group alias</p> <ul style="list-style-type: none"> <li>• &lt;HOST-IP&gt; – Specify the hosts' IP address.</li> <li>• &lt;HOST-IP&gt; – Optional. Specifies more than one host. A maximum of eight (8) hosts can be configured.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                             |
| network <NETWORK-ADDRESS/MASK><br>{<NETWORK-ADDRESS/MASK>}                            | <p>Associates a single or multiple networks with this network-group alias</p> <ul style="list-style-type: none"> <li>• &lt;NETWORK-ADDRESS/MASK&gt; – Specify the network's address and mask.</li> <li>• &lt;NETWORK-ADDRESS/MASK&gt; – Optional. Specifies more than one network. A maximum of eight (8) networks can be configured.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                 |

```
alias network-service <NETWORK-SERVICE-ALIAS-NAME> proto [<0-254>|<WORD>|eigrp|gre|igmp|
igmp|ospf|vrrp] {(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|ntp|pop3|
proto|sip|smtp|sourceport [<1-65535>|<WORD>]|ssh|telnet|tftp|www)}
```

|                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>alias network-service &lt;NETWORK-SERVICE-ALIAS- NAME&gt;</pre>                                                                                                                  | <p>Creates a network-service alias for this RF Domain. Or associates an existing network-service alias with this RF Domain. A network-service alias maps a name to network services and the corresponding source and destination software ports.</p> <ul style="list-style-type: none"> <li>• &lt;NETWORK-SERVICE-ALIAS-NAME&gt; – Specify a network-service alias name.</li> </ul> <p><b>Note:</b> Alias name should begin with '\$'.</p> <p><b>Note:</b> Aliases defined at any given level can be overridden at the next lower levels. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <pre>proto [&lt;0-254&gt;  &lt;WORD&gt;  eigrp gre  igmp igmp ospf vrrp]</pre>                                                                                                        | <p>Use one of the following options to associate an Internet protocol with this network-service alias:</p> <ul style="list-style-type: none"> <li>• &lt;0-254&gt; – Identifies the protocol by its number. Specify the protocol number from 0 - 254. This is the number by which the <i>protocol</i> is identified in the Protocol field of the IPv4 header and the Next Header field of IPv6 header. For example, the UDP (User Datagram Protocol's) designated number is 17.</li> <li>• &lt;WORD&gt; – Identifies the protocol by its name. Specify the protocol name.</li> <li>• eigrp – Selects EIGRP (Enhanced Interior Gateway Routing Protocol). The protocol number 88.</li> <li>• gre – Selects GRE (Generic Routing Encapsulation). The protocol number is 47.</li> <li>• igmp – Selects IGMP (Internet Group Management Protocol). The protocol number is 2.</li> <li>• igp – Selects IGP (Interior Gateway Protocol). The protocol number is 9.</li> <li>• ospf – Selects OSPF (Open Shortest Path First). The protocol number is 89.</li> <li>• vrrp – Selects VRRP (Virtual Router Redundancy Protocol). The protocol number is 112.</li> </ul>                                |
| <pre>&lt;1-65535&gt; &lt;WORD&gt;  bgp dns  ftp ftp-data  gopher https ldap  nntp  ntp pop3 proto sip smtp  sourceport [&lt;1-65535&gt;  &lt;WORD&gt;]] ssh telnet  tftp  www}}</pre> | <p>After specifying the protocol, you may configure a destination port for this service. These keywords are recursive and you can configure multiple protocols and associate multiple destination and source ports.</p> <ul style="list-style-type: none"> <li>• &lt;1-65535&gt; – Optional. Configures a destination port number from 1 - 65535</li> <li>• &lt;WORD&gt; – Optional. Identifies the destination port by the service name provided. For example, the SSH service uses TCP port 22.</li> <li>• bgp – Optional. Configures the default BGP (Border Gateway Protocol) services port (179)</li> <li>• dns – Optional. Configures the default DNS (Domain Name System) services port (53)</li> <li>• ftp – Optional. Configures the default FTP (File Transfer Protocol) control services port (21)</li> <li>• ftp-data – Optional. Configures the default FTP data services port (20)</li> <li>• gopher – Optional. Configures the default gopher services port (70)</li> <li>• https – Optional. Configures the default HTTPS services port (443)</li> <li>• ldap – Optional. Configures the default LDAP (Lightweight Directory Access Protocol) services port (389)</li> </ul> |

- nntp – Optional. Configures the default Newsgroup (NNTP) services port (119)
- ntp – Optional. Configures the default NTP (Network Time Protocol) services port (123)
- POP3 – Optional. Configures the default POP3 (Post Office Protocol) services port (110)
- proto – Optional. Use this option to select another Internet protocol in addition to the one selected in the previous step.
- sip – Optional. Configures the default SIP (Session Initiation Protocol) services port (5060)
- smtp – Optional. Configures the default SMTP (Simple Mail Transfer Protocol) services port (25)
- sourceport [<1-65535>|<WORD>] – Optional. After specifying the destination port, you may specify a single or range of source ports.
  - <1-65535> – Specify the source port from 1 - 65535.
  - <WORD> – Specify the source port range, for example 1-10.
- ssh – Optional. Configures the default SSH services port (22)
- telnet – Optional. Configures the default Telnet services port (23)
- tftp – Optional. Configures the default TFTP (Trivial File Transfer Protocol) services port (69)
- www – Optional. Configures the default HTTP services port (80)

`alias number <NUMBER-ALIAS-NAME> <0-4294967295>`

`alias number <NUMBER-ALIAS-NAME> <0-4294967295>` Creates a new number alias or applies an existing number, identified by the <NUMBER-ALIAS-NAME> keyword

- <NUMBER-ALIAS-NAME> – Specify the number alias name.
  - <0-4294967295> – Specify the number, from 0 - 4294967295, assigned to the number alias created.

Number aliases map a name to a numeric value. For example, 'alias number \$NUMBER 100'.

- The number alias name is: \$NUMBER
- The value assigned is: 100

The value referenced by alias \$NUMBER, wherever used, is 100.

`alias string <STRING-ALIAS-NAME> <LINE>`

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| alias string<br><STRING-<br>ALIAS-<br>NAME> | <p>Creates a string alias for this RF Domain. Or associates an existing string alias with this RF Domain. String aliases map a name to an arbitrary string value. For example, 'alias string \$DOMAIN test.example_company.com'. In this example, the string alias name is: \$DOMAIN and the string value it is mapped to is: test.example_company.com. In this example, the string alias refers to a domain name.</p> <ul style="list-style-type: none"> <li>• &lt;VLAN-ALIAS-NAME&gt; - Specify the string alias name. <ul style="list-style-type: none"> <li>• &lt;LINE&gt; - Specify the string value.</li> </ul> </li> </ul> <p><b>Note:</b> Alias name should begin with '\$'.</p> <p><b>Note:</b> Aliases defined at any given level can be overridden at the next lower levels. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence.</p> |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
alias vlan <VLAN-ALIAS-NAME> <1-4094>
```

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| alias vlan<br><VLAN-<br>ALIAS-NAME> | <p>Creates a VLAN alias for this RF Domain. Or associates an existing VLAN alias with this RF Domain. A VLAN alias maps a name to a VLAN ID.</p> <ul style="list-style-type: none"> <li>• &lt;VLAN-ALIAS-NAME&gt; - Specify the VLAN alias name.</li> </ul> <p><b>Note:</b> Alias name should begin with '\$'.</p>                                                                                            |
| <1-4094>                            | <p>Maps the VLAN alias to a VLAN ID</p> <ul style="list-style-type: none"> <li>• &lt;1-4094&gt; - Specify the VLAN ID from 1 - 4094.</li> </ul> <p><b>Note:</b> Aliases defined at any given level can be overridden at the next lower levels. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence.</p> |

### Examples

```
rfs4000-229D58(config)#show context
!
! Configuration of RFS4000 version 5.9.2.0-008B
!
!
version 2.5
!
!
alias network-group $TestNetGrpAlias network 192.168.13.0/24 192.168.16.0/24
alias network-group $TestNetGrpAlias address-range 192.168.13.7 to 192.168.13.16
192.168.13.20 to 192.168.13.25
!
alias network $TestNetworkAlias 192.168.13.0/24
!
alias host $TestHostAlias 192.168.13.10
!
alias address-range $TestAddRanAlias 192.168.13.10 to 192.168.13.13
!
alias network-service $NetworkServAlias proto udp
!
alias network-service $kerberos proto tcp 749 750 80 proto udp 68 sourceport 67
!
alias vlan $TestVLANAlias 1
--More--
rfs4000-229D58(config)#
```



In the following examples the global aliases '\$kerberos' and '\$TestVLANAlias' are associated with the RF Domain 'test' and overrides applied:

```
rfs4000-229D588(config-rf-domain-test)#alias network-service $kerberos proto tcp
749 750 80
rfs4000-229D58(config-rf-domain-test)#alias vlan $TestVLANAlias 10
rfs4000-229D58(config-rf-domain-test)#show context
rf-domain test
 no country-code
 alias network-service $kerberos proto tcp 749 750 80
 alias vlan $TestVLANAlias 10
rfs4000-229D58(config-rf-domain-test)#
nx9500-6C8809(config-rf-domain-test)#alias string $test example_company.com
nx9500-6C8809(config-rf-domain-test)#show context
rf-domain test
 no country-code
 alias string $test example_company.com
nx9500-6C8809(config-rf-domain-test)#
Example 1:
```

In the following examples, the network-group alias '\$test' is configured to include hosts 192.168.1.10 and 192.168.1.11, networks 192.168.2.0/24 and 192.168.3.0/24 and address-range 192.168.4.10 to 192.168.4.20.

```
rfs4000-229D58(config)#alias network-group $test host 192.168.1.10 192.168.1.11
rfs4000-229D58(config)#alias network-group $test network 192.168.2.0/24 192.168.3.0/24
rfs4000-229D58(config)#alias network-group $test address-range 192.168.4.10 to 192.168.4.20
```

Associate this network-group alias '\$test' to the RF Domain 'test' and override the 'host' element of the alias.

```
rfs4000-229D58(config-rf-domain-test)#alias network-group $test host 192.168.10.10
rfs4000-229D58(config-rf-domain-test)#alias network-group $test host 192.168.10.10
rfs4000-229D58(config-rf-domain-test)#show context
rf-domain test
 no country-code
 alias network-service $kerberos proto tcp 749 750 80
 alias network-group $test host 192.168.10.10
 alias network-group $test network 192.168.2.0/24 192.168.3.0/24
 alias network-group $test address-range 192.168.4.10 to 192.168.4.20
 alias vlan $TestVLANAlias 10
rfs4000-229D58(config-rf-domain-test)#
```

In the preceding example, the 'host' element of the network-group alias '\$test' has been overridden. But the 'network' and 'address-range' elements have been retained as is.

#### Related Commands

|                                                                                                        |
|--------------------------------------------------------------------------------------------------------|
| <b>no</b> Removes a network, network-group, network-service, VLAN, or string alias from this RF Domain |
|--------------------------------------------------------------------------------------------------------|

#### channel-list

Configures the channel list advertised by the AP radios. This command also enables dynamic update of a channel list.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
channel-list [2.4GHz|5GHz|dynamic]
channel-list dynamic
channel-list [2.4GHz|5GHz] <CHANNEL-LIST>
```

## Parameters

```
channel-list dynamic
```

|         |                                            |
|---------|--------------------------------------------|
| dynamic | Enables dynamic update of the channel list |
|---------|--------------------------------------------|

```
channel-list [2.4GHz|5GHz] <CHANNEL-LIST>
```

|                       |                                                                                                                                                                                                                    |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2.4GHz <CHANNEL-LIST> | Configures the channel list advertised by radios operating in the 2.4 GHz band <ul style="list-style-type: none"><li>&lt;CHANNEL-LIST&gt; – Specify the list of channels separated by commas or hyphens.</li></ul> |
| 5GHz <CHANNEL-LIST>   | Configures the channel list advertised by radios operating in the 5.0 GHz mode <ul style="list-style-type: none"><li>&lt;CHANNEL-LIST&gt; – Specify the list of channels separated by commas or hyphens.</li></ul> |

## Examples

```
nx9500-6C8809(config-rf-domain-default)#channel-list 2.4GHz 1-10
nx9500-6C8809(config-rf-domain-default)#show context
rf-domain default
no country-code
channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
nx9500-6C8809(config-rf-domain-default)#
```

## Related Commands

|    |                                                                                                                                                  |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------|
| no | Removes the list of channels configured on the selected RF Domain for 2.4 GHz and 5.0 GHz bands. Also disables dynamic update of a channel list. |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------|

## contact

Configures the network administrator's contact details. The network administrator is responsible for addressing problems impacting the network.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
contact <WORD>
```

## Parameters

```
contact <WORD>
```

|                |                                                   |
|----------------|---------------------------------------------------|
| contact <WORD> | Specify contact details, such as name and number. |
|----------------|---------------------------------------------------|

## Examples

```
nx9500-6C8809(config-rf-domain-default)#contact Bob+14082778691
nx9500-6C8809(config-rf-domain-default)#show context
rf-domain default
contact Bob+14082778691
```

```
no country-code
channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
nx9500-6C8809(config-rf-domain-default)#
```

#### Related Commands

|           |                                                     |
|-----------|-----------------------------------------------------|
| <b>no</b> | Removes the network administrator's contact details |
|-----------|-----------------------------------------------------|

### control-vlan

Configures the VLAN designated for traffic control in this RF Domain

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
control-vlan [<1-4094>|<VLAN-ALIAS-NAME>]
```

#### Parameters

```
control-vlan [<1-4094>|<VLAN-ALIAS-NAME>]
```

|                                           |                                                                                                                                                                         |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| control-vlan [<1-4094> <VLAN-ALIAS-NAME>] | Specify the VLAN ID from 1 - 4094. Alternately, use a vlan-alias to identify the control VLAN. If using a vlan-alias, ensure that the alias is existing and configured. |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config-rf-domain-default)#control-vlan 1
nx9500-6C8809(config-rf-domain-default)#show context
rf-domain default
 contact Bob+14082778691
 no country-code
 channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
 control-vlan 1
nx9500-6C8809(config-rf-domain-default)#
```

#### Related Commands

|           |                                                                |
|-----------|----------------------------------------------------------------|
| <b>no</b> | Disables the VLAN designated for controlling RF Domain traffic |
|-----------|----------------------------------------------------------------|

### controller-managed

Configures the adopting controller (wireless controller, Access Point, or service platform) as this RF Domain's manager. In other words, the RF Domain is controller managed, and the managing controller is the device managing the RF Domain.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
controller-managed
```

## Parameters

None

## Examples

```
rfs4000-229D58(config-rf-domain-test)#controller-managed
rfs4000-229D58(config-rf-domain-test)#show context
rf-domain test
 country-code in
controller-managed
 network-alias techPubs host 192.168.13.8
 network-alias techPubs address-range 192.168.13.10 to 192.168.13.15
 service-alias testing index 10 proto 9 destination-port range 21 21
rfs4000-229D58(config-rf-domain-test)#
```

## Related Commands

|                                                                                           |
|-------------------------------------------------------------------------------------------|
| <b>no</b> Removes the adopting controller or service platform as this RF Domain's manager |
|-------------------------------------------------------------------------------------------|

## country-code

Configures a RF Domain's country of operation. Since device channels transmit in specific channels unique to the country of operation, it is essential to configure the country code correctly or risk using illegal operation.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
country-code <WORD>
```

## Parameters

```
country-code <WORD>
```

|              |                                                   |
|--------------|---------------------------------------------------|
| country-code | Configures the RF Domain's country of operation   |
| <WORD>       | Specify the two (2) letter ISO-3166 country code. |

## Examples

```
nx9500-6C8809nx9500-6C8809(config-rf-domain-default)#country-code ?
WORD The 2 letter ISO-3166 country code
ae United Arab Emirates
ag Antigua and Barbuda
ai Anguilla
al Albania
an Dutch Antilles
ar Argentina
at Austria
au Australia
ba Bosnia-Herzegovina
bb Barbados
bd Bangladesh
be Belgium
bf Burkina Faso
```

```
--More--
nx9500-6C8809(config-rf-domain-default)#
nx9500-6C8809(config-rf-domain-default)#country-code us
nx9500-6C8809(config-rf-domain-default)#show context
rf-domain default
 contact Bob+14082778691
 country-code us
 channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
 control-vlan 1
nx9500-6C8809(config-rf-domain-default)#
```

#### Related Commands

|           |                                                                    |
|-----------|--------------------------------------------------------------------|
| <b>no</b> | Removes or resets this RF Domain's configured country of operation |
|-----------|--------------------------------------------------------------------|

#### geo-coordinates

Configures the longitude and latitude of the RF Domain in order to fix its exact geographical location on a map. Use this command to define the geographical area where a common set of device configurations are deployed and managed by this RF Domain policy.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
geo-coordinates <-90.0000-90.0000> <-180.0000-180.0000>
```

#### Parameters

```
geo-coordinates <-90.0000-90.0000> <-180.0000-180.0000>
```

|                                                               |                                                                                                                                                                                                                                                                |
|---------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| geo-coordinates<br><-90.0000-90.0000><br><-180.0000-180.0000> | Configures the geo-coordinates of this RF Domain <ul style="list-style-type: none"> <li>• &lt;-90.0000-90.0000&gt; - Specify the latitude from -90.0000 - 90.0000.</li> <li>• -180.0000-180.0000 - Specify the longitude from -180.0000 - 180.0000.</li> </ul> |
|---------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config-rf-domain-TechPubs)#geo-coordinates 12.971599 77.594563
nx9500-6C8809(config-rf-domain-TechPubs)#show context
rf-domain TechPubs
 location Bangalore
 geo-coordinates 12.9716 77.5946
 timezone Asia/Calcutta
 country-code in
 use database-policy default
 use nsight-policy AP-rfd
 control-vlan 1
 controller-managed
 use license WEBF
nx9500-6C8809(config-rf-domain-TechPubs)#
```

#### Related Commands

|           |                                                               |
|-----------|---------------------------------------------------------------|
| <b>no</b> | Removes or resets this RF Domain's configured geo-coordinates |
|-----------|---------------------------------------------------------------|

#### layout

Configures the RF Domain's layout in terms of area, floor, and location on a map. It allows users to place APs across the deployment map. A maximum of 256 layouts is permitted.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
layout [area|description|floor|map-location] {(area/description/floor/map-location)}
layout [area <AREA-NAME>|description <LINE>|floor <FLOOR-NAME> {<1-4094>}|
map-location <URL> units [feet|meters]] {(area <AREA-NAME>/description <LINE>/
floor <FLOOR-NAME> {<1-4094>}/map-location <URL> units [feet|meters])}
```

#### Parameters

```
layout [area <AREA-NAME>|description <LINE>|floor <FLOOR-NAME> {<1-4094>}|
map-location <URL> units [feet|meters]] {(area <AREA-NAME>/description <LINE>/
floor <FLOOR-NAME> {<1-4094>}/map-location <URL> units [feet|meters])}
```

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| layout                                 | Configures the RF Domain's layout in terms of area, floor, and location on a map<br>These are recursive parameters and you can configure one or all of these parameters.                                                                                                                                                                                                                                                                                                                                                                                                           |
| area <AREA-NAME>                       | Configures the RF Domain's layout in terms of the area of location <ul style="list-style-type: none"> <li>• &lt;AREA-NAME&gt; – Specify the area name.</li> </ul> <p>After configuring the RF Domain's area of functioning, optionally specify the floor name (and number), description, and/or the location on map.</p>                                                                                                                                                                                                                                                           |
| description <LINE>                     | Configures a description for this RF Domain <ul style="list-style-type: none"> <li>• &lt;LINE&gt; – Specify a description that enables you to identify the RF Domain. For a multi-worded string, use double quotes.</li> </ul>                                                                                                                                                                                                                                                                                                                                                     |
| floor <FLOOR-NAME> <1-4094>            | Configures the RF Domain's layout in terms of the floor name and number <ul style="list-style-type: none"> <li>• &lt;FLOOR-NAME&gt; – Specify the floor name.</li> <li>• &lt;1-4094&gt; – Optional. Specifies the floor number from 1 - 4094. The default floor number is 1.</li> </ul> <p>After configuring the RF Domain's floor name (and number), optionally specify the area name, description, and/or the location on map.</p>                                                                                                                                               |
| map-location <URL> units [feet meters] | Configures the location of the RF Domain on the map <ul style="list-style-type: none"> <li>• &lt;URL&gt; – Specify the URL to configure the map location.</li> <li>• units [feet meters] – Configures the map units. The options are: feet or meters <ul style="list-style-type: none"> <li>feet – Configures the map units in terms of feet</li> <li>meters – Configures the map units in terms of meter</li> </ul> </li> </ul> <p>After configuring the location of the RF Domain on the map, optionally specify the area name, floor name (and number), and/or description.</p> |

#### Examples

```
nx9500-6C8809(config-rf-domain-default)#layout map-location www.firstfloor.com units
meters area HamiltonAve floor Floor1
nx9500-6C8809(config-rf-domain-default)#show context
rf-domain default
contact Bob+14082778691
country-code us
channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
layout area HamiltonAve floor Floor1 map-location www.firstfloor.com units meters
```

```
control-vlan 1
nx9500-6C8809(config-rf-domain-default)#
```

#### Related Commands

|                 |                                        |
|-----------------|----------------------------------------|
| <code>no</code> | Removes the RF Domain's layout details |
|-----------------|----------------------------------------|

#### location

Configures the RF Domain's physical location. The location could be as specific as the building name or floor number. Or it could be generic and include an entire site. The location defines the physical area where a common set of device configurations are deployed and managed by a RF Domain policy.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
location <WORD>
```

#### Parameters

```
location <WORD>
```

|                                    |                                                                                                                                                                               |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>location &lt;WORD&gt;</code> | Configures the RF Domain location by specifying the area or building name <ul style="list-style-type: none"><li>• <code>&lt;WORD&gt;</code> - Specify the location.</li></ul> |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config-rf-domain-default)#location SanJose
nx9500-6C8809(config-rf-domain-default)#show context
rf-domain default
 location SanJose
 contact Bob+14082778691
 country-code us
 channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
 layout area Ecospace floor Floor1 map-location www.firstfloor.com units meters
 control-vlan 1
nx9500-6C8809(config-rf-domain-default)#
```

#### Related Commands

|                 |                                  |
|-----------------|----------------------------------|
| <code>no</code> | Removes the RF Domain's location |
|-----------------|----------------------------------|

#### location-server

Configures the ExtremeLocation server's IP address or hostname on the selected RF Domain. When configured, the AP 7522, AP 7532, AP 7562, AP 8432 and AP 8533 model access points, within the RF Domain, extract and forward client-location related data to the specified ExtremeLocation server.

ExtremeLocation is a highly scalable indoor locationing platform that gathers location-related analytics, such as visitor trends, peak and off-peak times, dwell time, heat-maps, etc. to enable entrepreneurs deeper visibility at a venue. To enable the location tracking system, the ExtremeLocation server should be up and running and the RF Domain configuration should point to the ExtremeLocation server.

Supported in the following platforms:

- Service Platforms — NX 7510, NX 95XX, NX 96XX

#### Syntax

```
location-server 1 ip <EL-SERVER-IP/HOSTNAME> {port <1-65535>}
```

#### Parameters

```
location-server 1 ip <IP/HOSTNAME> {port <1-65535>}
```

|                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>location-server 1 ip &lt;IP/ HOSTNAME&gt;</pre> | <p>Identifies the ExtremeLocation server by its hostname</p> <ul style="list-style-type: none"> <li>• 1 – Sets the server ID as 1. As of now only one ExtremeLocation server is configurable.</li> <li>• ip &lt;IP/HOSTNAME&gt; – Enter ExtremeLocation server’s hostname. This is the ExtremeLocation server designated to receive RSSI scan data from a WiNG dedicated sensor.</li> </ul> <p><b>Note:</b> Enter the server’s hostname and not the IP address, as the IP address is likely to change periodically in order to balance load across multiple Location server instances.</p> |
| <pre>port &lt;1-65535&gt;</pre>                      | <p>Optional. Configures the port where the ExtremeLocation server is reachable.</p> <ul style="list-style-type: none"> <li>• &lt;1-65535&gt; – Specify a port from 1 - 65535.</li> </ul> <p><b>Note:</b> By default the ExtremeLocation server is reachable on port 443.</p>                                                                                                                                                                                                                                                                                                               |

#### Examples

```
nx9500-6C8809(config-rf-domain-test)#location-server 1 ip 1.2.3.4 port 200
nx9500-6C8809(config-rf-domain-test)#show context
rf-domain test
no country-code
location-server 1 ip 1.2.3.4 port 200
nx9500-6C8809(config-rf-domain-test)#
```

#### Related Commands

|               |                                                   |
|---------------|---------------------------------------------------|
| <pre>no</pre> | Removes the ExtremeLocation server configurations |
|---------------|---------------------------------------------------|

#### location-tenantid

Configures the ExtremeLocation Tenant’s account number.

ExtremeLocation Tenants, at the time of registration, are communicated (via, email) an account number uniquely identifying the Tenant. Configure this account number in the RF Domain context. When configured, RF Domain AP reports, pushed to the ExtremeLocation server, include the Tenant’s account number along with the reporting AP’s MAC address. Including the Tenant account number reinforces the Tenant’s identity.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
location-tenantid <WORD>
```



## Parameters

location-tenantid <WORD>

|                          |                                                                                                                                                     |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| location-tenantid <WORD> | Configures the ExtremeLocation Tenant's account number <ul style="list-style-type: none"><li>• &lt;WORD&gt; - Specify the account number.</li></ul> |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-rf-domain-ExLocTenant1)#location-tenantid 123456
nx9500-6C8809(config-rf-domain-ExLocTenant1)#location-tenantid
testTenant123nx9500-6C8809(config-rf-domain-ExLocTenant1)#show context
rf-domain ExLocTenant1
country-code us
location-tenantid 123456
nx9500-6C8809(config-rf-domain-ExLocTenant1)#
```

## Related Commands

|                                               |                                                                                 |
|-----------------------------------------------|---------------------------------------------------------------------------------|
| <b>no (rf-domain-config-mode)</b> on page 526 | Removes the ExtremeLocation Tenant's account number configured on the RF Domain |
|-----------------------------------------------|---------------------------------------------------------------------------------|

## mac-name

Configures a relevant name for each MAC address. Use this command to associate client names to specific connected client MAC addresses for improved client management.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

mac-name <MAC> <NAME>

## Parameters

mac-name <MAC> <NAME>

|                       |                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mac-name <MAC> <NAME> | Assigns a user-friendly name to this RF Domain's member access point's connected client to assist in its easy recognition <ul style="list-style-type: none"><li>• &lt;MAC&gt; - Specify the MAC address</li><li>• &lt;NAME&gt; - Specify the client name for the specified MAC address. The name specified here will be used in events and statistics.</li></ul> |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-rf-domain-default)#mac-name 11-22-33-44-55-66 TestDevice
nx9500-6C8809(config-rf-domain-default)#show context
rf-domain default
location SanJose
contact Bob+14082778691
country-code us
channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
mac-name 11-22-33-44-55-66 TestDevice
layout area Ecospace floor Floor1 map-location www.firstfloor.com units meters
control-vlan 1
nx9500-6C8809(config-rf-domain-default)#
```

## Related Commands

|                 |                                         |
|-----------------|-----------------------------------------|
| <code>no</code> | Removes the MAC address to name mapping |
|-----------------|-----------------------------------------|

### override-smart-rf

Enables dynamic channel switching for Smart RF radios. This command allows you to configure an override list of channels that Smart RF can use for channel compensations on 2.4 GHz and 5.0 GHz radios.

When a radio fails or is faulty, a Smart RF policy provides automatic recovery by instructing neighboring access points to increase their transmit power to compensate for the coverage loss. Once correct access point placement has been established, Smart-RF can optionally be leveraged for automatic detector radio selection. Smart-RF uses detector radios to monitor RF events and can ensure availability of adequate detector coverage.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
override-smartrf channel-list [2.4GHz|5GHz] <CHANNEL-LIST>
```

### Parameters

```
override-smartrf channel-list [2.4GHz|5GHz] <CHANNEL-LIST>
```

|                                          |                                                                                                                                                                                   |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>override-smartrf</code>            | Enables dynamic channel switching for Smart RF radios                                                                                                                             |
| <code>channel-list</code>                | Configures a list of channels for 2.4 GHz and 5.0 GHz Smart RF radios                                                                                                             |
| <code>2.4GHz &lt;CHANNEL-LIST&gt;</code> | Selects the 2.4 GHz Smart RF radio channels <ul style="list-style-type: none"><li>• <code>&lt;CHANNEL-LIST&gt;</code> – Specify a list of channels separated by commas.</li></ul> |
| <code>5GHz &lt;CHANNEL-LIST&gt;</code>   | Selects the 5.0 GHz Smart RF radio channels <ul style="list-style-type: none"><li>• <code>&lt;CHANNEL-LIST&gt;</code> – Specify a list of channels separated by commas.</li></ul> |

### Examples

```
nx9500-6C8809(config-rf-domain-default)#override-smartrf channel-list 2.4GHz 1,2,3
nx9500-6C8809(config-rf-domain-default)#show context
rf-domain default
 contact Bob+14082778691
 country-code us
 override-smartrf channel-list 2.4GHz 1,2,3
 layout area Eospace floor Floor1 map-location www.firstfloor.com units meters
nx9500-6C8809(config-rf-domain-default)#
```

## Related Commands

|                 |                                                                                         |
|-----------------|-----------------------------------------------------------------------------------------|
| <code>no</code> | Removes the override-smartrf list of channels configured for 2.4 GHz and 5.0 GHz radios |
|-----------------|-----------------------------------------------------------------------------------------|

### override-wlan

Configures RF Domain level overrides for a WLAN

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
override-wlan <WLAN-NAME> [shutdown|ssid|template|vlan-pool|wep128|wpa-wpa2-psk]
override-wlan <WLAN-NAME> [shutdown|ssid <SSID>|template <TEMPLATE-NAME>|vlan-pool
<1-4094> {limit <0-8192>}]
override-wlan <WLAN-NAME> wpa-wpa2-psk [0 <WORD>|2 <WORD>]
override-wlan <WLAN-NAME> wep128 [key <1-4> hex [0 <WORD>|2 <WORD>]|transmit-key <1-4>]
```

#### Parameters

```
override-wlan <WLAN-NAME> [shutdown|ssid <SSID>|template <TEMPLATE-NAME>|vlan-pool
<1-4094> {limit <0-8192>}]
```

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <WLAN-NAME>                         | Configures the WLAN name<br>If applying RF Domain level overrides to an existing WLAN, specify its name. If creating a new WLAN, specify a name not exceeding 32 characters and representing the WLAN's coverage area. After creating the WLAN, configure its override parameters.                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| shutdown                            | Shuts down WLAN operation on all mapped radios                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| ssid <SSID>                         | Configures a override SSID associated with this WLAN <ul style="list-style-type: none"> <li>• &lt;SSID&gt; – Specify the SSID (should not exceed 32 characters in length).</li> </ul> <p>Each WLAN provides associated wireless clients with a SSID. This has limitations, because it requires wireless clients to associate with different SSIDs to obtain QoS and security policies. However, a WiNG-managed RF Domain can have WLANs assigned and advertise a single SSID, and yet allow users to inherit different QoS or security policies.</p>                                                                                                                                                                                   |
| template <TEMPLATE-NAME>            | Configures a template name for this RF Domain <ul style="list-style-type: none"> <li>• &lt;TEMPLATE-NAME&gt; – Specify the template name (should not exceed 32 characters in length).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| vlan-pool <1-4094> {limit <0-8192>} | Configures the override VLANs available to this WLAN <ul style="list-style-type: none"> <li>• &lt;1-4094&gt; – Specify the VLAN ID from 1 - 4094.</li> <li>• limit &lt;0-8192&gt; – Optional. Sets a limit to the number of users on this VLAN from 0 - 8192. The default is 0.</li> </ul> <p>Controllers and service platforms allow the mapping of a WLAN to more than one VLAN. Wireless clients associating with a WLAN are assigned VLANs, from the pool representative of the WLAN, in a way that ensures proper load balancing across VLANs. Clients are tracked per VLAN, and assigned to the least used/loaded VLAN. Client VLAN usage is tracked on a per-WLAN basis. The maximum allowed client limit is 8192 per VLAN.</p> |

```
override-wlan <WLAN-NAME> wpa-wpa2-psk [0 <WORD>|2 <WORD>]
```

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <WLAN-NAME>                  | Configures the WLAN name<br>If applying RF Domain level overrides to an existing WLAN, specify its name. If creating a new WLAN, specify a name not exceeding 32 characters and representing the WLAN's coverage area. After creating the WLAN, configure its override parameters.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| wpa-wpa2-psk<br><PASSPHRASE> | Overrides a WLAN's existing WPA-WPA2 pre-shared key or passphrase at the RF Domain level. WPA2 is a newer 802.11i standard that provides wireless security that is stronger than WPA (Wi-Fi Protected Access) and WEP. <ul style="list-style-type: none"> <li>• &lt;PASSPHRASE&gt; - Specify a WPA-WPA2 key or passphrase. It is an alphanumeric string of 8 to 64 ASCII characters or 64 HEX characters as the primary string, which both the transmitting and receiving authenticators must share in this new override PSK. The alphanumeric string allows character spaces. The string is converted to a numeric value. This passphrase saves the you the necessity of entering the 256-bit key each time keys are generated.</li> </ul> |

```
override-wlan <WLAN-NAME> wep128 [key <1-4> hex [0 <WORD>|2 <WORD>]|transmit-key <1-4>]
```

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <WLAN-NAME>                       | Configures the WLAN name<br>If applying RF Domain level overrides to an existing WLAN, specify its name. If creating a new WLAN, specify a name not exceeding 32 characters and representing the WLAN's coverage area. After creating the WLAN, configure its override parameters.                                                                                                                                                                                                                                                                                                        |
| wep128                            | Overrides a WLAN's existing WEP128 keys at the RF Domain level (not the profile level). WEP128 uses a 104 bit key, which is concatenated with a 24-bit initialization vector (IV) to form the RC4 traffic key. WEP may be all a small-business user needs for the simple encryption of wireless data on the WLAN. However, networks that require more security are at risk from a WEP flaw. WEP is only recommended if there are client devices incapable of using higher forms of security. The existing 802.11 standard alone offers administrators no effective method to update keys. |
| key <1-4> hex [0 <WORD> 2 <WORD>] | Configures the WEP128 key. A total of four keys can be configured. <ul style="list-style-type: none"> <li>• &lt;1-4&gt; - Select the key index from 1- 4. <ul style="list-style-type: none"> <li>• hex - Configures a hexadecimal key <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specify the WEP128/Keyguard key (should not exceed 26 hexadecimal characters in length).</li> </ul> </li> </ul> </li> </ul>                                                                                                                                                                 |
| transmit-key <1-4>                | Configures transmit WEP/Keyguard key settings <ul style="list-style-type: none"> <li>• &lt;1-4&gt; - Transmit the key identified by the key index specified here. Specify the index from 1 - 4.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                |

### Examples

```
nx9500-6C8809(config-rf-domain-default)#override-wlan test vlan-pool 2 limit 20
nx9500-6C8809(config-rf-domain-default)#show context
rf-domain default
contact Bob+14082778691
country-code us
override-smartrf channel-list 2.4GHz 1,2,3
override-wlan test vlan-pool 2 limit 20
layout area Ecospace floor Floor1 map-location www.firstfloor.com units meters
nx9500-6C8809(config-rf-domain-default)#
```

### Related Commands

|    |                                              |
|----|----------------------------------------------|
| no | Resets the override WLAN settings to default |
|----|----------------------------------------------|

sensor-server

Configures an AirDefense sensor server on this RF Domain. Sensor servers allow network administrators to monitor and download data from multiple sensors remote locations using Ethernet TCP/IP or serial communications. This enables administrators to respond quickly to interferences and coverage problems.

WIPS (*Wireless Intrusion Protection System*) protects the controller managed network, wireless clients and Access Point radio traffic from attacks and unauthorized access. WIPS provides tools for standards compliance and around-the-clock wireless network security in a distributed environment. WIPS allows administrators to identify and accurately locate attacks, rogue devices and network vulnerabilities in real time and permits both a wired and wireless lockdown of wireless device connections upon acknowledgement of a threat.

In addition to dedicated AirDefense sensors, an access point radio can function as a sensor and upload information to a dedicated WIPS server (external to the controller). Unique WIPS server configurations can be used by RF Domains to ensure a WIPS server configuration is available to support the unique data protection needs of individual RF Domains.

WIPS is not supported on a WLAN basis, rather sensor functionality is supported on the access point radio(s) available to each controller managed WLAN. When an access point radio is functioning as a WIPS sensor, it is able to scan in sensor mode across all legal channels within the 2.4 and 5.0 GHz bands. Sensor support requires a AirDefense WIPS Server on the network. Sensor functionality is not provided by the access point alone. The access point works in conjunction with a dedicated WIPS server.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
sensor-server <1-3> ip <IP/HOSTNAME> {port [443|<1-65535>]}
```

#### Parameters

```
sensor-server <1-3> ip <IP/HOSTNAME> {port [443|<1-65535>]}
```

|                      |                                                                                                                                                                                                                                                                                                  |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sensor-server <1-3>  | Configures the AirDefense sensor server parameters <ul style="list-style-type: none"> <li>• &lt;1-3&gt; - Select the server ID from 1 - 3. The server with the lowest defined ID is reached first. The default is 1.</li> </ul>                                                                  |
| ip <IP/HOSTNAME>     | Configures the (non DNS) IPv4 address of the sensor server <ul style="list-style-type: none"> <li>• &lt;IP/HOSTNAME&gt; - Specify the sensor server's IPv4 address or hostname.</li> </ul>                                                                                                       |
| port [443 <1-65535>] | Optional. Configures the sensor server port. The options are: <ul style="list-style-type: none"> <li>• 443 - Configures port 443, the default port used by the AirDefense server</li> <li>• &lt;1-6553&gt; - Allows you to select a WIPS/AirDefense sensor server port from 1 - 65535</li> </ul> |

#### Examples

```
nx9500-6C8809(config-rf-domain-default)#sensor-server 2 ip 172.16.10.3 port 443
nx9500-6C8809(config-rf-domain-default)#show context
rf-domain default
contact Bob+14082778691
country-code us
```

```

sensor-server 2 ip 172.16.10.3
override-smarttrf channel-list 2.4GHz 1,2,3
override-wlan test vlan-pool 2 limit 20
layout area Ecospace floor Floor1 map-location www.firstfloor.com units meters
nx9500-6C8809(config-rf-domain-default)#

```

#### Related Commands

|           |                                                  |
|-----------|--------------------------------------------------|
| <b>no</b> | Disables the AirDefense sensor server parameters |
|-----------|--------------------------------------------------|

#### stats

Configures settings that define how RF Domain statistics are updated

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```

stats update-interval
stats update-interval [<5-300>|auto]

```

#### Parameters

```

stats update-interval [<5-300>|auto]

```

|                                   |                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| stats                             | Configures stats related settings on this RF Domain                                                                                                                                                                                                                                                                                        |
| update-interval<br>[<5-300> auto] | Configures the interval at which RF Domain statistics are updated. The options are: <ul style="list-style-type: none"> <li>• &lt;5-300&gt; – Specify an update interval from 5 - 300 seconds.</li> <li>• auto – The RF Domain manager automatically adjusts the update interval based on the load. This is the default setting.</li> </ul> |

#### Examples

```

nx9500-6C8809(config-rf-domain-default)#stats update-interval 200
nx9500-6C8809(config-rf-domain-default)#show context
rf-domain default
contact Bob+14082778691
stats update-interval 200
country-code us
sensor-server 2 ip 172.16.10.3
override-smarttrf channel-list 2.4GHz 1,2,3
override-wlan test vlan-pool 2 limit 20
layout area Ecospace floor Floor1 map-location www.firstfloor.com units meters
nx9500-6C8809(config-rf-domain-default)#

```

#### Related Commands

|           |                               |
|-----------|-------------------------------|
| <b>no</b> | Resets stats related settings |
|-----------|-------------------------------|

#### timezone

Configures the RF Domain's geographic time zone. By default all WiNG devices are shipped with the time zone and time format set to UTC (Universal Time Coordinated) and 24-hour clock respectively. If the time zone is not reset, all devices within the RF Domain will display time relative to the UTC - Greenwich Time. Resetting the time zone is recommended, especially for RF Domains deployed across different geographical locations. The time zone can either be set on a specific device or on an RF

Domain. When configured as RF Domain setting, it applies to all devices within the domain. For more information on configuring the time zone on a device, see [timezone](#) on page 1282 (device config mode).

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
timezone <TIMEZONE>
```

#### Parameters

```
timezone <TIMEZONE>
```

|                 |                                                                                                                      |
|-----------------|----------------------------------------------------------------------------------------------------------------------|
| time <TIMEZONE> | Specify the RF Domain's time zone. The configured time zone will apply to all devices within the selected RF Domain. |
|-----------------|----------------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config-rf-domain-default)#timezone America/Los_Angeles
nx9500-6C8809(config-rf-domain-default)#show context
rf-domain default
 contact Bob+14082778691
 timezone America/Los_Angeles
 stats update-interval 200
 country-code us
 sensor-server 2 ip 172.16.10.3
 override-smartrf channel-list 2.4GHz 1,2,3
 override-wlan test vlan-pool 2 limit 20
 layout area Ecospace floor Floor1 map-location www.firstfloor.com units meters
nx9500-6C8809(config-rf-domain-default)#
```

Use [TAB] to view the built-in timezones.

```
nx9500-6C8809(config-rf-domain-test)#timezone <TAB>
Africa/ Asia/ Atlantic/ Australia/ CET CST6CDT
EET EST5EDT Etc/ Europe/ MST7MDT Pacific/
PST8PDT US/ America/
nx9500-6C8809(config-rf-domain-test)#
```

Each of these time zones are further differentiated into sub time zones. For example, as shown in the following example:

```
nx9500-6C8809(config-rf-domain-test)#timezone Africa/
Africa/Cairo Africa/Casablanca Africa/Harare
Africa/Johannesburg Africa/Lagos Africa/Nairobi
nx9500-6C8809(config-rf-domain-test)#
```

#### Related Commands

|    |                                 |
|----|---------------------------------|
| no | Removes a RF Domain's time zone |
|----|---------------------------------|

#### tree-node

Configures the hierarchical (tree-node) structure under which this RF Domain is located

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533

- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
tree-node [campus|city|country|region] {(campus|city|country|region)}
```

### Parameters

```
tree-node [campus|city|country|region] {(campus|city|country|region)}
```

|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| tree-node | Configures the hierarchical tree structure defining the RF Domain's location. The tree node hierarchy can be configured in any order, but will always appear as: country > region > city > campus. Further, a higher node, such as country, cannot be defined under a lower node, such as region. An RF Domain can be placed under any one of the tree nodes. But, an RF Domain at the country level may have all four nodes defined. Whereas, an RF Domain restricted to a campus, cannot have the country, city, and region nodes. At least one of these four nodes must be defined. This feature is disabled by default. |
| campus    | Configures the campus name for this RF Domain                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| city      | Configures the city for this RF Domain                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| country   | Configures the country for this RF Domain                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| region    | Configures the region for this RF Domain                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

### Usage Guidelines

The following points need to be taken into consideration when creating the tree-node structure:

- Adding a *country* first is a good idea since region, city, and campus can all be added as sub-nodes in the tree structure. However, the selected country is an invalid tree node until a RF Domain is mapped.
- A *city* and *campus* can be added in the tree structure as sub-nodes under a region. An RF Domain can be mapped anywhere down the hierarchy for a region and not just directly under a country. For example, a region can have city, campus, and one RF Domain mapped.
- Only a campus can be added as a sub-node under a city. The city is an invalid tree node until a RF Domain is mapped somewhere within the directory tree.
- A campus is the last node in the hierarchy before a RF Domain, and it is not valid unless it has a RF Domain mapped.
- After creating the tree structure do a commit and save for the tree configuration to take effect and persist across reboots.

### Examples

```
rfs4000-229D58(config-rf-domain-test)#tree-node campus EcoSpace City Bangalore
country India region South
rfs4000-229D58(config-rf-domain-test)#
rfs4000-229D58(config-rf-domain-test)#show context
rf-domain test
country-code in
tree-node country India region South city Bangalore campus EcoSpace
rfs4000-229D58(config-rf-domain-test)#
```

### Related Commands

|    |                                                 |
|----|-------------------------------------------------|
| no | Removes the RF Domain's tree-node configuration |
|----|-------------------------------------------------|

use (rf-domain-config-mode)



Associates the following with an RF Domain: database policy, NSight policy, sensor policy, Smart RF policy, WIPS policy, RTL server policy, and Web filtering license.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
use [database-policy|license|nsight-policy|rtl-server-policy|sensor-policy|
smart-rf-policy|wips-policy]
use [database-policy <DATABASE-POLICY-NAME>|license <WEB-FILTERING-LICENSE>|
nsight-policy <NSIGHT-POLICY-NAME>|rtl-server-policy <RTL-SERVER-POLICY-NAME>|
sensor-policy <SENSOR-POLICY-NAME>|smart-rf-policy <SMART-RF-POLICY-NAME>|
wips-policy <WIPS-POLICY-NAME>]
```

#### Parameters

```
use [database-policy <DATABASE-POLICY-NAME>|license <WEB-FILTERING-LICENSE>|
nsight-policy <NSIGHT-POLICY-NAME>|rtl-server-policy <RTL-SERVER-POLICY-NAME>|
sensor-policy <SENSOR-POLICY-NAME>|smart-rf-policy <SMART-RF-POLICY-NAME>|
wips-policy <WIPS-POLICY-NAME>]
```

|                                            |                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| use                                        | Associates the following policies with the RF Domain: database policy, NSight policy, sensor policy, Smart RF policy, WIPS policy. It also applies a Web filtering license to the selected RF Domain.                                                                                                                                            |
| database-policy <DATABASE-POLICY-NAME>     | Associates a database policy with the selected RF Domain <ul style="list-style-type: none"> <li>• &lt;DATABASE-POLICY-NAME&gt; - Specify the database policy name (should be existing and configured).</li> </ul>                                                                                                                                |
| license <WEB-FILTERING-LICENSE>            | Obtains the specified Web filtering license from the adopting controller <ul style="list-style-type: none"> <li>• &lt;WEB-FILTERING-LICENSE&gt; - Specify the WEBF license name.</li> </ul>                                                                                                                                                      |
| nsight-policy <NSIGHT-POLICY-NAME>         | Associates an NSight policy with the selected RF Domain <ul style="list-style-type: none"> <li>• Specify the NSight policy name (should be existing and configured). When applied, it enables the RF Domain manager to gather statistical data from access points within the domain and forward to the NOC running the NSight server.</li> </ul> |
| rtl-server-policy <RTL-SERVER-POLICY-NAME> | Associates an RTL (Real Time Locationing) server policy with the selected RF Domain <ul style="list-style-type: none"> <li>• &lt;RTL-SERVER-POLICY-NAME&gt; - Specify the RTL server policy name (should be existing and configured)</li> </ul>                                                                                                  |
| sensor-policy <SENSOR-POLICY-NAME>         | Associates a sensor policy with the selected RF Domain <ul style="list-style-type: none"> <li>• &lt;SENSOR-POLICY-NAME&gt; - Specify the sensor policy name (should be existing and configured).</li> </ul>                                                                                                                                      |

|                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| smart-rf-policy<br><SMART-RF-POLICY-NAME> | <p>Associates a Smart RF policy with the selected RF Domain. When associated, the Smart RF policy provides automatic recovery from coverage loss (due to failed or faulty radio) by instructing neighboring access points to increase their transmit power. Once correct access point placement has been established, Smart-RF can optionally be leveraged for automatic detector radio selection. Smart-RF uses detector radios to monitor RF events to ensure availability of adequate detector coverage.</p> <ul style="list-style-type: none"> <li>• &lt;SMART-RF-POLICY-NAME&gt; – Specify the Smart RF policy name (should be existing and configured).</li> </ul> |
| wips-policy <WIPS-POLICY-NAME>            | <p>Associates a WIPS policy with the selected RF Domain. A WIPS policy provides protection against wireless threats and acts as a key layer of security complementing wireless VPNs, encryption and authentication. A WIPS policy uses a dedicated sensor for actively detecting and locating rogue AP devices. After detection, WIPS uses mitigation techniques to block the devices by manual termination, air lockdown, or port suppression.</p> <ul style="list-style-type: none"> <li>• &lt;WIPS-POLICY-NAME&gt; – Specify the WIPS policy name (should be existing and configured).</li> </ul>                                                                     |

### Examples

```

nx9500-6C8809(config-rf-domain-default)#use smart-rf-policy Smart-RF1
nx9500-6C8809(config-rf-domain-default)#use wips-policy WIPS1
nx9500-6C8809(config-rf-domain-default)#show context
rf-domain default
 contact Bob+14082778691
 timezone America/Los_Angeles
 stats update-interval 200
 country-code us
 use smart-rf-policy Smart-RF1
 use wips-policy WIPS1
 sensor-server 2 ip 172.16.10.3
 override-smartrf channel-list 2.4GHz 1,2,3
 override-wlan test vlan-pool 2 limit 20
 layout area Ecospace floor Floor1 map-location www.firstfloor.com units meters
nx9500-6C8809(config-rf-domain-default)#

```

### Related Commands

|    |                                          |
|----|------------------------------------------|
| no | Resets profiles used with this RF Domain |
|----|------------------------------------------|

### no (rf-domain-config-mode)

Negates a command or reverts configured settings to their default. When used in the RF Domain context, the no command removes the RF Domain settings, or reverts them to default values.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
no [alias|channel-list|contact|control-vlan|controller-managed|country-code|
geo-coordinates|layout|location|location-server|location-tenantid|mac-name|
```

```

nsight-sensor|override-smartrf|override-wlan|sensor-server|stats|timezone|tree-node|
use]
no [channel-list [2.4GHz|5GHz|dynamic]|contact|control-vlan|controller-managed|
country-code|location-server 1|location-tenantid|mac-name <MAC>|
nsight-sensor|sensor-server <1-3>|stats update-interval|timezone|tree-node]
no alias [address-range|host|network|network-group [address-range|host|network]|
network-service|number|string|vlan] <ALIAS-NAME>
no layout {(area <AREA-NAME>/floor <FLOOR-NAME>)}
no override-smartrf channel-list [2.4GHz|5GHz]
no override-wlan <WLAN-NAME> [shutdown|ssid|template|vlan-pool [<1-4094>|all]|
wep128 [key <1-3>|transmit-key]|wpa-wpa2-psk]
no use [database-policy|license|nsight-policy|rtl-server-policy|sensor-policy|
smart-rf-policy|wips-policy]

```

#### Parameters

```
no <PARAMETERS>
```

|                 |                                                                             |
|-----------------|-----------------------------------------------------------------------------|
| no <PARAMETERS> | Removes or reverts this RF Domain's settings based on the parameters passed |
|-----------------|-----------------------------------------------------------------------------|

#### Examples

The following example shows the default RF Domain settings before the 'no' commands are executed:

```

nx9500-6C8809(config-rf-domain-default)#show context
rf-domain default
 location SanJose
 contact Bob+14082778691
 country-code us
 channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
 mac-name 11-22-33-44-55-66 TestDevice
 layout area Ecospace floor Floor1 map-location www.firstfloor.com units meters
 control-vlan 1
nx9500-6C8809(config-rf-domain-default)#
nx9500-6C8809(config-rf-domain-default)#no channel-list 2.4GHz 1-10
nx9500-6C8809(config-rf-domain-default)#no mac-name 11-22-33-44-55-66
nx9500-6C8809(config-rf-domain-default)#no location
nx9500-6C8809(config-rf-domain-default)#no control-vlan

```

The following example shows the default RF Domain settings after the 'no' commands are executed:

```

nx9500-6C8809(config-rf-domain-default)#show context
rf-domain default
 contact Bob+14082778691
 country-code us
 layout area Ecospace floor Floor1 map-location www.firstfloor.com units meters
nx9500-6C8809(config-rf-domain-default)#

```

#### *rfs4000*

Adds an RFS 4000 wireless controller to the network

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
rfs4000 <DEVICE-RFS4000-MAC>
```

## Parameters

rfs4000 <DEVICE-RFS4000-MAC>

|                     |                                     |
|---------------------|-------------------------------------|
| <DEVICE-RFS4000-MAC | Specify the RFS 4000's MAC address. |
|---------------------|-------------------------------------|

## Examples

```
nx9500-6C8809(config)#rfs4000 10-20-30-40-50-60
nx9500-6C8809(config-device-10-20-30-40-50-60)#
```

## Related Commands

|    |                                                          |
|----|----------------------------------------------------------|
| no | Removes an RFS 4000 wireless controller from the network |
|----|----------------------------------------------------------|

### *nx5500*

Adds an integrated NX 5500 series service platform to the network. If a profile for this service platform is not available, a new profile is created.

#### **Supported in the following platforms:**

- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

## Syntax

nx5500 <DEVICE-NX5500-MAC>

## Parameters

nx5500 <DEVICE-NX5500-MAC>

|                     |                                                                 |
|---------------------|-----------------------------------------------------------------|
| <DEVICE-NX5500-MAC> | Specifies the MAC address of a NX 5500 series service platform. |
|---------------------|-----------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config)#nx5500 B4-C7-02-3C-FA-6E
nx9500-6C8809(config-device-B4-C7-02-3C-FA-6E)#
```

## Related Commands

|    |                                                            |
|----|------------------------------------------------------------|
| no | Removes a NX 5500 series service platform from the network |
|----|------------------------------------------------------------|

### *nx75xx*

Adds an integrated NX 75XX series service platform to the network. If a profile for service platform is not available, a new profile is created.

#### **Supported in the following platforms:**

- Service Platforms — NX 7500, NX 9500, NX 9510

## Syntax

nx75xx <DEVICE-NX75XX-MAC>

## Parameters

`nx75xx <DEVICE-NX75XX-MAC>`

|                                        |                                                                  |
|----------------------------------------|------------------------------------------------------------------|
| <code>&lt;DEVICE-NX75XX-MAC&gt;</code> | Specifies the MAC address of the NX 75XX series service platform |
|----------------------------------------|------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config)#nx75xx B4-C9-81-6C-FA-7C
nx9500-6C8809(config-device-B4-C9-81-6C-FA-7C)#show context
nx75xx B4-C9-81-6C-FA-7C
 use profile default-nx75xx
 use rf-domain default
 hostname nx75xx-6CFA7C
nx9500-6C8809(config-device-B4-C9-81-6C-FA-7C)#
nx75xx-6CFA7C>show adoption status
Adopted by:
Type : nx9000
System Name : nx9500-6C8809
MAC address : B4-C7-99-6C-88-09
MiNT address : 19.6C.88.09
Time : 1 days 01:57:50 ago
```

Adopted Devices:

| DEVICE-NAME   | VERSION      | CFG-STAT   | MSG | ADOPTED-BY    | LAST-ADOPTION   | UPTIME          |
|---------------|--------------|------------|-----|---------------|-----------------|-----------------|
| ap7161-11E6C4 | 5.9.2.0-008B | configured | No  | nx75xx-6CFA7C | 1 days 01:49:44 | 1 days 01:59:34 |

Total number of devices displayed: 1  
nx75xx-6CFA7C>

## Related Commands

|                 |                                                             |
|-----------------|-------------------------------------------------------------|
| <code>no</code> | Removes an NX 75XX series service platform from the network |
|-----------------|-------------------------------------------------------------|

## *nx9000*

Adds an NX9XXX (NX95XX and NX96XX) series service platform to the network

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

## Syntax

`nx9000 <DEVICE-NX9XXX-MAC>`

## Parameters

`nx9000 <DEVICE-NX9XXX-MAC>`

|                                        |                                                                |
|----------------------------------------|----------------------------------------------------------------|
| <code>&lt;DEVICE-NX9XXX-MAC&gt;</code> | Specifies the MAC address of a NX9XXX series service platform. |
|----------------------------------------|----------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config)#nx9000 B4-C7-89-7C-81-08
nx9500-6C8809(config-device-B4-C7-89-7C-81-08)#
```

## Related Commands

|                 |                                                           |
|-----------------|-----------------------------------------------------------|
| <code>no</code> | Removes a NX9XXX series service platform from the network |
|-----------------|-----------------------------------------------------------|

### *roaming-assist-policy*

Configures a roaming assist policy that enables access points to assist wireless clients in making roaming decisions, such as which access point to connect, etc.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
roaming-assist-policy <ROAMING-ASSIST-POLICY-NAME>
```

#### Parameters

```
roaming-assist-policy <ROAMING-ASSIST-POLICY-NAME>
```

|                              |                                                                                      |
|------------------------------|--------------------------------------------------------------------------------------|
| <ROAMING-ASSIST-POLICY-NAME> | Specify the roaming-assist policy name. If the policy does not exist, it is created. |
|------------------------------|--------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config)#roaming-assist-policy test
nx9500-6C8809(config-roaming-assist-policy-test)#?
```

Roaming Assist Mode commands:

|                                  |                                                                                    |
|----------------------------------|------------------------------------------------------------------------------------|
| <code>action</code>              | Configure action - action is death / log / assisted-roam                           |
| <code>aggressiveness</code>      | Configure the roaming aggressiveness for a wireless client                         |
| <code>detection-threshold</code> | Configure the detection threshold - when exceeded, client monitoring starts        |
| <code>disassoc-time</code>       | Configure the disassociation time - time after which a disassociation is sent      |
| <code>handoff-count</code>       | Configure the handoff count - number of times client can exceed handoff threshold  |
| <code>handoff-threshold</code>   | Configure the handoff threshold - when exceeds an action is taken.                 |
| <code>monitoring-interval</code> | Configure the monitoring interval - interval at which client monitoring occurs     |
| <code>no</code>                  | Negate a command or set its defaults                                               |
| <code>sampling-interval</code>   | Configure the sampling interval - interval at which client rssi values are checked |
| <code>clrscr</code>              | Clears the display screen                                                          |
| <code>commit</code>              | Commit all changes made in this session                                            |
| <code>end</code>                 | End current mode and change to EXEC mode                                           |
| <code>exit</code>                | End current mode and down to previous mode                                         |
| <code>help</code>                | Description of the interactive help system                                         |
| <code>revert</code>              | Revert changes                                                                     |
| <code>service</code>             | Service Commands                                                                   |
| <code>show</code>                | Show running system information                                                    |
| <code>write</code>               | Write running configuration to memory or terminal                                  |

```
nx9500-6C8809(config-roaming-assist-policy-test)#
```

## Related Commands

|                 |                                           |
|-----------------|-------------------------------------------|
| <code>no</code> | Removes an existing roaming-assist-policy |
|-----------------|-------------------------------------------|



### Note

For more information on the Roaming Assist Policy commands, [ROAMING-ASSIST-POLICY](#).

## *role-policy*

Creates a role-based firewall policy and enters its configuration mode

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
role-policy <ROLE-POLICY-NAME>
```

### Parameters

```
role-policy <ROLE-POLICY-NAME>
```

|                                       |                                                                                                  |
|---------------------------------------|--------------------------------------------------------------------------------------------------|
| <code>&lt;ROLE-POLICY-NAME&gt;</code> | Specify the role policy name. If a policy with the specified name does not exist, it is created. |
|---------------------------------------|--------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config)#role-policy role1
nx9500-6C8809(config-role-policy-role1)#?
Role Policy Mode commands:
 default-role Configuration for Wireless Clients not matching any role
 ldap-deadperiod Ldap dead period interval
 ldap-query Set the ldap query mode
 ldap-server Add a ldap server
 ldap-timeout Ldap query timeout interval
 no Negate a command or set its defaults
 user-role Create a role

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-role-policy-role1)#
```

## Related Commands

`no` Removes an existing role policy



### Note

For more information on Role Policy commands, see [ROLE-POLICY](#).

## *route-map*

Creates a dynamic BGP (Border Gateway Protocol) route map and enters its configuration mode

BGP route maps are used by network administrators to define rules controlling redistribution of routes between routers and routing processes. These route maps are also used to control and modify routing information.

### Supported in the following platforms:

- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

### Syntax

```
route-map <ROUTE-MAP-NAME>
```

### Parameters

```
route-map <ROUTE-MAP-NAME>
```

`route-map <ROUTE-MAP-NAME>` Creates a new BGP route map and enters its configuration mode

### Examples

```
nx9500-6C8809(config)#route-map test
nx9500-6C8809(config-dr-route-map-test)#?
Route Map Mode commands:
deny Add a deny route map rule to deny set operations
no Negate a command or set its defaults
permit Add a permit route map rule to permit set operations

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

nx9500-6C8809(config-dr-route-map-test)#
```

## Related Commands

`no` Removes an existing dynamic BGP route map



### Note

For more information on BGP route maps, see [BORDER GATEWAY PROTOCOL](#) on page 1852.



## *routing-policy*

Creates a routing policy and enters its configuration mode

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
routing-policy <ROUTING-POLICY-NAME>
```

### Parameters

```
routing-policy <ROUTING-POLICY-NAME>
```

|                       |                                                                            |
|-----------------------|----------------------------------------------------------------------------|
| <ROUTING-POLICY-NAME> | Specify the role policy name. If the policy does not exist, it is created. |
|-----------------------|----------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config)#routing-policy test
nx9500-6C8809(config-routing-policy-test)#?
Routing Policy Mode commands:
 apply-to-local-packets Use Policy Based Routing for packets generated by
 the device
 logging Enable logging for this Route Map
 no Negate a command or set its defaults
 route-map Create a Route Map
 use Set setting to use

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-routing-policy-test)#
```

### Related Commands

|    |                                    |
|----|------------------------------------|
| no | Removes an existing routing policy |
|----|------------------------------------|



#### Note

For more information on Routing Policy commands, see [ROUTING-POLICY](#).

## *rtl-server-policy*

Creates an RTL server policy and enters its configuration mode. When configured and applied on an access point (AP 7522, AP 7532, AP 8432, AP 8533), this policy enables the sending of RSSI feeds from

the access point to a server. The RTL server policy provides the exact location (URL) of the server. The RSSI feeds sent are as per the sensor-policy configured and applied on the access point. Therefore, ensure that a sensor-policy, with the rssi-interval-duration specified, is existing, configured, and applied on the access points.

To initiate RSSI feed posts to the Euclid locationing server, use the RTL server policy on the:

- AP's device/profile context, or
- AP's RF Domain context.

**Supported in the following platforms:**

- Access Points — AP 7522, AP 7532, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX VX 9000

**Syntax**

```
rtl-server-policy <RTL-POLICY-NAME>
```

**Parameters**

```
rtl-server-policy <RTL-POLICY-NAME>
```

|                                      |                                                                                                                    |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <code>&lt;RTL-POLICY-NAME&gt;</code> | Specify the RTL server policy name. If an RTL server policy with the specified name does not exist, it is created. |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------|

```
nx9500-6C8809(config)#rtl-server-policy test
nx9500-6C8809(config-rtl-server-policy-test)#?
RTL Server Policy Mode commands:
no Negate a command or set its defaults
url Configure the url to send the real time RSSI feed to

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal
```

```
nx9500-6C8809(config-rtl-server-policy-test)#
```

|                                                                           |                                                                                                                                                                                                                            |
|---------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>no</code>                                                           | Removes an existing RTL server policy                                                                                                                                                                                      |
| <code>use</code> on page 1232 (profile/device configuration mode command) | Documents the 'use' command in a device's profile or device configuration context. Use this option to associate this RTL server policy to an access point's profile or device.                                             |
| <code>use</code> (RF Domain configuration mode command)                   | Documents the 'use' command in the RF Domain configuration context. Use this option to associate this RTL server policy to an RF Domain. When associated, the policy is applied to all access points within the RF Domain. |

**rtl-server-policy-config-commands**

The following table summarizes the RTL server policy configuration mode commands:

**Table 27: RTL Server Policy Config Mode Commands**

| Command                      | Description                                |
|------------------------------|--------------------------------------------|
| <code>url</code> on page 535 | Configures the RTL server's URL            |
| <code>no</code> on page 535  | Removes the RTL server's URL configuration |

url

Configures the RTL server's exact location. This is the URL at which the server can be reached.

Supported in the following platforms:

- Access Points — AP 7522, AP 7532, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX VX 9000

Syntax

`url <URL>`

Parameters

`url <URL>`

|                              |                                                                                                                               |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <code>url &lt;URL&gt;</code> | Configures the RTL server's URL <ul style="list-style-type: none"><li>• <code>&lt;URL&gt;</code> - Specify the URL.</li></ul> |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------|

Examples

```
nx9500-6C8809(config-rtl-server-policy-test)#url https://testrtlserver.com
nx9500-6C8809(config-rtl-server-policy-test)#show context
rtl-server-policy test
 url https://testrtlserver.com
nx9500-6C8809(config-rtl-server-policy-test)#
```

Related Commands

|                             |                                         |
|-----------------------------|-----------------------------------------|
| <code>no</code> on page 535 | Removes the RTL server's configured URL |
|-----------------------------|-----------------------------------------|

no

Removes the locationing server's URL configuration

Supported in the following platforms:

- Access Points — AP 7522, AP 7532, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX VX 9000

Syntax

`no <URL>`

Parameters

`no <URL>`

|                             |                              |
|-----------------------------|------------------------------|
| <code>no &lt;URL&gt;</code> | Removes the RTL server's URL |
|-----------------------------|------------------------------|

Examples

The following example displays the RTL server policy 'test' settings before the 'no' command is executed:

```
nx9500-6C8809(config-rtl-server-policy-test)#show context
rtl-server-policy test
 url https://testrtlserver.com
nx9500-6C8809(config-rtl-server-policy-test)#
nx9500-6C8809(config-rtl-server-policy-test)#no url
```

The following example displays the RTL server policy 'test' settings after the 'no' command is executed:

```
nx9500-6C8809(config-rtl-server-policy-test)#show context
rtl-server-policy test
nx9500-6C8809(config-rtl-server-policy-test)#
```

#### Related Commands

|                             |                                         |
|-----------------------------|-----------------------------------------|
| <code>no</code> on page 535 | Removes the RTL server's configured URL |
|-----------------------------|-----------------------------------------|

### *schedule-policy*

Creates a schedule policy and enters its configuration mode. A schedule policy strategically enforces application filter policy rules during administrator assigned intervals.

#### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
schedule-policy <SCHEDULE-POLICY-NAME>
```

#### Parameters

```
schedule-policy <SCHEDULE-POLICY-NAME>
```

|                                                           |                                                                                                                                    |
|-----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| <code>schedule-policy &lt;SCHEDULE-POLICY-NAME&gt;</code> | Specify the Schedule policy name. If the policy does not exist, it is created. The name should not exceed 32 characters in length. |
|-----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config)#schedule-policy test
nx9500-6C8809(config-schedule-policy-test)#?
Schedule Policy Mode commands:
 description Schedule policy description
 no Negate a command or set its defaults
 time-rule Configure a time rule

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-schedule-policy-test)#
```

## Related Commands

|                 |                                     |
|-----------------|-------------------------------------|
| <code>no</code> | Removes an existing schedule policy |
|-----------------|-------------------------------------|

## schedule-policy-config-commands

The following table summarizes schedule-policy configuration mode commands:

**Table 28: Schedule Policy Config Mode Commands**

| Command                              | Description                                                                                                                        |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| <code>description</code> on page 537 | Configures a description for this schedule policy that differentiates it from other policies with similar time rule configurations |
| <code>time-rule</code> on page 537   | Configures a time rule specifying the days and optionally the start and end times                                                  |
| <code>no</code> on page 538          | Removes the selected schedule policy's settings                                                                                    |

### description

Configures a description for this schedule policy that differentiates it from other policies with similar time rule configurations

Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
description <WORD>
```

#### Parameters

```
description <WORD>
```

|                                       |                                                                                                                                                                                                                                                                                            |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>description &lt;WORD&gt;</code> | Configures this schedule policy's description <ul style="list-style-type: none"><li>• <code>&lt;WORD&gt;</code> - Enter a description not exceeding 80 characters in length. The description should uniquely identify the policy from other policies with similar configuration.</li></ul> |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config-schedule-policy-test)#description "Denies social networking sites on weekdays."
nx9500-6C8809(config-schedule-policy-test)#show context
schedule-policy test
 description "Denies social networking sites on weekdays."
nx9500-6C8809(config-schedule-policy-test)#
```

### Related Commands

|                             |                                                        |
|-----------------------------|--------------------------------------------------------|
| <code>no</code> on page 538 | Removes or modifies this schedule policy's description |
|-----------------------------|--------------------------------------------------------|

### time-rule

Configures a time rule specifying the days and optionally the start and end times. When applied to an application-policy rule, the schedule policy defines the enforcement time of the rule. For more information, see [application-policy](#) on page 267.

Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

### Syntax

```
time-rule days [sunday|monday|tuesday|wednesday|thursday|friday|saturday|all|weekends|weekdays] {start-time <HH:MM> [end-time <HH:MM>]}
```

### Parameters

```
time-rule days [sunday|monday|tuesday|wednesday|thursday|friday|saturday|all|weekends|weekdays] {start-time <HH:MM> [end-time <HH:MM>]}
```

|                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| time-rule                                                                                  | Configures a time rule in days and hours and minutes<br>A schedule policy can have more than one non-overlapping time-rules. The following time-rules, having overlapping time periods, are invalid: 'weekdays, start-time 9:30 am, end-time 11:30 pm' and 'all, start-time 12:00 am, end-time 12:00 pm'.                                                                                                                                                                                                                                                                                                                                  |
| days [sunday monday  tuesday  wednesday thursday friday  saturday all] weekends  weekdays] | Specifies the days on which the time rule is applicable <ul style="list-style-type: none"><li>• sunday – Applicable on Sundays only</li><li>• monday – Applicable on Mondays only</li><li>• tuesday – Applicable on Tuesdays only</li><li>• wednesday – Applicable on Wednesdays only</li><li>• thursday – Applicable on Thursdays only</li><li>• friday – Applicable on Fridays only</li><li>• saturday – Applicable on Saturdays only</li><li>• weekends – Applicable on weekends only</li><li>• weekdays – Applicable on weekdays only</li><li>• all – Applicable on all days</li></ul>                                                 |
| start-time <HH:MM> [end-time <HH:MM>]                                                      | After specifying the days of enforcement, specify the following: <ul style="list-style-type: none"><li>• start-time – Optional. Specifies the enforcement start time<ul style="list-style-type: none"><li>• &lt;HH:MM&gt; – Specify the start time in hours and minutes in the HH:MM format.</li></ul></li></ul> If no start time is specified, the time rule is enforced, on the specified days, at all time. <ul style="list-style-type: none"><li>• end-time – Specifies the enforcement end time<ul style="list-style-type: none"><li>• &lt;HH:MM&gt; – Specify the time in hours and minutes in the HH:MM format.</li></ul></li></ul> |

### Examples

```
nx9500-6C8809(config-schedule-policy-test)#time-rule days weekdays start-time 10:00 end-time 23:30
nx9500-6C8809(config-schedule-policy-test)#show context
schedule-policy test
 description "Denies social networking sites on weekdays."
 time-rule days weekdays start-time 10:00 end-time 23:30
nx9500-6C8809(config-schedule-policy-test)#
```

### Related Commands

|                |                                                |
|----------------|------------------------------------------------|
| no on page 538 | Removes the time-rule from the schedule policy |
|----------------|------------------------------------------------|

no

Removes the selected schedule policy's settings

Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
no [description|time-rule]
no description
no time-rule days [sunday|monday|tuesday|wednesday|thursday|friday|saturday|
all|weekends|weekdays]
```

#### Parameters

```
no <PARAMETERS>
```

|                 |                                                                       |
|-----------------|-----------------------------------------------------------------------|
| no <PARAMETERS> | Removes the schedule policy's settings based on the parameters passed |
|-----------------|-----------------------------------------------------------------------|

#### Examples

The following example displays the schedule policy 'test' settings before the 'no' commands have been executed:

```
nx9500-6C8809(config-schedule-policy-test)#show context
schedule-policy test
 description "Denies social networking sites on weekdays."
 time-rule days weekdays start-time 10:00 end-time 23:30
nx9500-6C8809(config-schedule-policy-test)#
```

The following example displays the schedule policy 'test' settings after the 'no' commands have been executed:

```
nx9500-6C8809(config-schedule-policy-test)#no description
nx9500-6C8809(config-schedule-policy-test)#no time-rule days weekdays
nx9500-6C8809(config-schedule-policy-test)#show context
schedule-policy test
nx9500-6C8809(config-schedule-policy-test)#
```

#### Related Commands

|  |
|--|
|  |
|--|

#### *self*

Invokes the logged device's configuration context

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
self
```

#### Parameters

None

## Examples

```
nx9500-6C8809(config)#self
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```

### *sensor-policy*

Creates a sensor policy and enters its configuration mode.

Access point radios, functioning as sensors, along with AirDefense WIPS servers protect networks from attacks and unauthorized access. These access point sensors scan legal channels and (based on a WIPS policy settings) identify events potential threats to the managed network. These events are reported to the AirDefense WIPS server, which determines the action taken.

In addition to WIPS support, sensor functionality has now been added for the Extreme Network's locationing system. The ExtremeLocation system for Wi-Fi locationing includes WiNG controllers, and access points functioning as sensors. Within the Locationing architecture, sensors scan for RSSI data on an administrator-defined interval and send to a dedicated ExtremeLocation Server resource, as opposed to an ADSP server. The ExtremeLocation Server collects the RSSI data from WiNG sensor devices, and calculates the location of Wi-Fi devices for ExtremeLocation administrators.

Use this command to configure a policy defining the mode of scanning, the channels to scan (in case scan-mode is set to custom-scan), and the RSSI interval. For the sensor policy to take effect, use the policy either in the access point's RF Domain context or in the access point's device context.



#### Note

If a dedicated sensor is utilized with WIPS for rogue detection, any sensor policy used is discarded and not utilized by the sensor. To avoid this situation, use ADSP channel settings exclusively to configure the sensor and not the WiNG interface.

### Supported in the following platforms:

- Service Platforms — NX 7510, NX 95XX, NX 96XX, VX 9000

### Syntax

```
sensor-policy <SENSOR-POLICY-NAME>
```

### Parameters

```
sensor-policy <SENSOR-POLICY-NAME>
```

|                      |                                                                                                                                                                                                                                                                                                                                         |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <SENSOR-POLICY-NAME> | Specify the Sensor policy name. If a sensor policy with the specified name does not exist, it is created. The name should not exceed 32 characters in length. No character spaces are permitted within the name. Define a name unique to the policy's channel and scan mode configuration to help differentiate it from other policies. |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config)#sensor-policy test
nx9500-6C8809(config-sensor-policy-test)#?
Sensor Policy Mode commands:
 custom-scan Channel configuration in Custom Scan channels
 no Negate a command or set its defaults
 rssi-interval-duration Configure the periodicity of sending RSSI info from
 sensor to server
 scan-mode Configure the Scan mode
```



```

clearscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

```

```
nx9500-6C8809(config-sensor-policy-test)#
```

## Related Commands

|                 |                                   |
|-----------------|-----------------------------------|
| <code>no</code> | Removes an existing sensor policy |
|-----------------|-----------------------------------|

## sensor-policy-config-commands

The following table summarizes sensor-policy configuration mode commands:

**Table 29: Sensor Policy Config Mode Commands**

| Command                                        | Description                                                                                                                                            |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>custom-scan</code> on page 541           | Configures the channel scanning settings when the scan-mode is set to custom-scan                                                                      |
| <code>rss-interval-duration</code> on page 542 | Configures the interval at which dedicated sensors scan channels for RSSI assessments and send the collected data to a specified MPact server resource |
| <code>scan-mode</code> on page 543             | Configures the mode of scanning used by dedicated sensors (access point radios)                                                                        |
| <code>no</code> on page 544                    | Removes or reverts to default a sensor policy's settings                                                                                               |

### custom-scan

Configures the channel scanning settings when the scan-mode is set to custom-scan



#### Note

If the mode of scanning is set to Custom-Scan, use this command to configure the channels to be scanned. To set the mode of scanning to custom-scan, use the `scan-mode > Custom-Scan` command. For more information, see [scan-mode](#) on page 543.

Supported in the following platforms:

- Service Platforms — NX 7510, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
custom-scan channel-frequency <CHANNEL-FREQUENCY> width
[20MHz | 40MHz-Bth | 40MHz-Lower | 40MHz-Upper | 80MHz] scan-weight <SCAN-WEIGHT>
```

#### Parameters

```
custom-scan channel-frequency <CHANNEL-FREQUENCY> width
[20MHz | 40MHz-Bth | 40MHz-Lower | 40MHz-Upper | 80MHz] scan-weight <SCAN-WEIGHT>
```

|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| custom-scan                                                | Configures the custom-scan channel frequency, channel width, and scan weight                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| channel-frequency <CHANNEL-FREQUENCY>                      | Configures the channel frequency. A list of unique channels in the 2.4, 4.9, 5 and 6 GHz band can be collectively or individually enabled for customized channel scans and RSSI reporting. <ul style="list-style-type: none"> <li>• &lt;CHANNEL-FREQUENCY&gt; – Specify a single or multiple, ‘comma-separated’ channel frequencies.</li> </ul>                                                                                                                                                                                                                                         |
| width [20MHz  40MHz-Both  40MHz-Lower  40MHz-Upper  80MHz] | Configures the channel width. When custom channels are selected for RSSI scans, each selected channel can have its own width defined. Numerous channels have their width fixed at 20MHz, 802.11a radios support 20 and 40 MHz channel widths. <ul style="list-style-type: none"> <li>• 20MHz – Sets the channel width as 20 Mhz</li> <li>• 40Mhz-Both – Sets the channel width as 40Mhz-Both</li> <li>• 40Mhz-Lowe – Sets the channel width as 40Mhz-Lower</li> <li>• 40Mhz-Upper – Sets the channel width as 40Mhz-Upper</li> <li>• 80Mhz – Sets the channel width as 80Mhz</li> </ul> |
| scan-weight <SCAN-WEIGHT>                                  | Configures the scan-weight (scanning duration) for each of the selected channels. Each selected channel can have its weight prioritized in respect to the amount of time a scan is permitted within the defined RSSI scan interval. <ul style="list-style-type: none"> <li>• &lt;SCAN-WEIGHT&gt; – Specify the scan weightage given to each selected channel.</li> </ul>                                                                                                                                                                                                                |

### Examples

```

nx9500-6C8809(config-sensor-policy-test)#custom-scan channel-frequency 2412 width 20MHz
scan-weight 1000
nx9500-6C8809(config-sensor-policy-test)#custom-scan channel-frequency 2417 width 20MHz
scan-weight 1000
nx9500-6C8809(config-sensor-policy-test)#show context
sensor-policy test
 scan-mode Custom-Scan
 custom-scan channel-frequency 2412 width 20MHz scan-weight 1000
 custom-scan channel-frequency 2417 width 20MHz scan-weight 1000
nx9500-6C8809(config-sensor-policy-test)#

```

### Related Commands

|                |                                                                                               |
|----------------|-----------------------------------------------------------------------------------------------|
| no on page 544 | Removes channels from the channels-to-scan list in case of scan-mode being set to Custom-Scan |
|----------------|-----------------------------------------------------------------------------------------------|

### rssi-interval-duration

Configures the interval, in seconds, at which dedicated sensors scan channels for RSSI assessments and send the RSSI data obtained to a specified server resource

Supported in the following platforms:

- Service Platforms — NX 7510, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
rssi-interval-duration <1-60>
```

#### Parameters

```
rssi-interval-duration <1-60>
```

|                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>rsssi-interval-duration &lt;1-60&gt;</code> | <p>Configures the RSSI interval duration in seconds. This is the interval at which the sensor scans channels for RSSI data and forwards the data to a dedicated server resource. The server calculates real-time locations of Wi-Fi devices based on the this data.</p> <ul style="list-style-type: none"> <li><code>&lt;1-60&gt;</code> – Specify the RSSI interval duration from 1 - 60 seconds. The default is 1 second.</li> </ul> <p>The channels scanned for RSSI assessment depends on the scan-mode selected. For more information, see <a href="#">scan-mode</a> on page 543 and <a href="#">custom-scan</a> on page 541.</p> <p>Ensure that the server's IP address or hostname has been configured in the access point sensor's RF Domain context.</p> |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```

nx9500-6C8809(config-sensor-policy-test)#rsssi-interval-duration 30
nx9500-6C8809(config-sensor-policy-test)#show context
sensor-policy test
 rssi-interval-duration 30
 scan-mode Custom-Scan
 custom-scan channel-frequency 2412 width 20MHz scan-weight 1000
 custom-scan channel-frequency 2417 width 20MHz scan-weight 1000
nx9500-6C8809(config-sensor-policy-test)#

```

### Related Commands

|                                |                                                                                                                           |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <a href="#">no</a> on page 544 | Resets the interval at which RSSI data is collected and sent by the sensor to the MPact server host to default (1 second) |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------|

## scan-mode

Configures the mode of scanning used by dedicated sensors (access point radios)

Supported in the following platforms:

- Service Platforms — NX 7510, NX 95XX, NX 96XX, VX 9000

### Syntax

```

scan-mode [Channel-Lock|Custom-Scan|Default-Scan]
scan-mode Channel-Lock lock-frequency <LOCK-FREQUENCY>
scan-mode [Custom-Scan|Default-Scan]

```

### Parameters

```

scan-mode Channel-Lock lock-frequency <LOCK-FREQUENCY>

```

|                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>scan-mode</code>                                          | Configures the mode of scanning used by the sensors to scan system-defined or user-defined channels for RSSI assessments. The options are: Channel-Lock, Custom-Scan, and Default-Scan.                                                                                                                                                                                                                                         |
| <code>Channel-Lock lock-frequency &lt;LOCK-FREQUENCY&gt;</code> | Configures the mode of scanning as Channel-Lock <ul style="list-style-type: none"> <li><code>lock-frequency &lt;LOCK-FREQUENCY&gt;</code> – Locks scanning for RSSI data to one specific channel identified by the <code>&lt;LOCK-FREQUENCY&gt;</code> parameter.</li> <li><code>&lt;LOCK-FREQUENCY&gt;</code> – Specify the channel frequency in MHz. When specified, the sensor scans only this specified channel.</li> </ul> |

```

scan-mode [Custom-Scan|Default-Scan]

```

|              |                                                                                                                                                                                                                                                                                                                             |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| scan-mode    | Configures the mode of scanning used by the sensor. The options are: channel-lock, custom-scan, and default-scan.                                                                                                                                                                                                           |
| Custom-Scan  | Configures the mode of scanning as Custom-Scan<br>Select this option to restrict scanning to user-defined channels. If selecting this option, use the custom-scan > channel-frequency command to configure the channels scanned by the dedicated sensor. For more information, see <a href="#">custom-scan</a> on page 541. |
| Default-Scan | Configures the mode of scanning as Default-Scan. This is the default setting. By default the system has a fixed, built-in list of channels that are scanned. These channels are hard coded in a spread pattern of 1, 6, 11, 36, 40, 44, and 48. When selected, the dedicated sensor scans only these default channels.      |

### Examples

```

nx9500-6C8809(config-sensor-policy-test)#scan-mode Custom-Scan
nx9500-6C8809(config-sensor-policy-test)#show context
sensor-policy test
 rssi-interval-duration 30
 scan-mode Custom-Scan
 custom-scan channel-frequency 2412 width 20MHz scan-weight 1000
 custom-scan channel-frequency 2417 width 20MHz scan-weight 1000
nx9500-6C8809(config-sensor-policy-test)#

```

### Related Commands

|                                |                                                 |
|--------------------------------|-------------------------------------------------|
| <a href="#">no</a> on page 544 | Reverts the scan-mode to default (Default-Scan) |
|--------------------------------|-------------------------------------------------|

no

Removes or reverts to default a sensor policy's settings

Supported in the following platforms:

- Service Platforms — NX 7510, NX 95XX, NX 96XX, VX 9000

### Syntax

```

no [custom-scan|rssi-interval-duration|scan-mode]
no custom-scan channel-frequency <CHANNEL-FREQUENCY-LIST>
no rssi-interval-duration
no scan-mode

```

### Parameters

no <PARAMETERS>

|                 |                                                                                       |
|-----------------|---------------------------------------------------------------------------------------|
| no <PARAMETERS> | Removes or reverts to default a sensor policy settings based on the parameters passed |
|-----------------|---------------------------------------------------------------------------------------|

### Examples

The following example shows the sensor-policy 'test' settings before the 'no' commands are executed:

```

nx9500-6C8809(config-sensor-policy-test)#show context
sensor-policy test
 rssi-interval-duration 30
 scan-mode Custom-Scan
 custom-scan channel-frequency 2412 width 20MHz scan-weight 1000
 custom-scan channel-frequency 2417 width 20MHz scan-weight 1000
nx9500-6C8809(config-sensor-policy-test)#

```

The scan-mode is reverted back to the default setting of 'Default-Scan', as show in the following output:

```
nx9500-6C8809(config-sensor-policy-test)#no scan-mode
nx9500-6C8809(config-sensor-policy-test)#no custom-scan channel-frequency 2412
nx9500-6C8809(config-sensor-policy-test)#no custom-scan channel-frequency 2417
nx9500-6C8809(config-sensor-policy-test)#show context
sensor-policy test
 rssi-interval-duration 30
 scan-mode Default-Scan
nx9500-6C8809(config-sensor-policy-test)#
```

### smart-rf-policy

Configures a Smart RF policy and enters its configuration mode

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
smart-rf-policy <SMART-RF-POLICY-NAME>
```

#### Parameters

```
smart-rf-policy <SMART-RF-POLICY-NAME>
```

|                        |                                                                                                      |
|------------------------|------------------------------------------------------------------------------------------------------|
| <SMART-RF-POLICY-NAME> | Specify the Smart RF policy name. If a policy with the specified name does not exist, it is created. |
|------------------------|------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config)#smart-rf-policy test
nx9500-6C8809(config-smart-rf-policy-test)#?
Smart RF Mode commands:
 area Specify channel list/ power for an area
 assignable-power Specify the assignable power during power-assignment
 avoidance-time Time to avoid a channel once dfs/adaptivity
 avoidance is necessary
 channel-list Select channel list for smart-rf
 channel-width Select channel width for smart-rf
 coverage-hole-recovery Recover from coverage hole
 enable Enable this smart-rf policy
 group-by Configure grouping parameters
 interference-recovery Recover issues due to excessive noise and
 interference
 neighbor-recovery Recover issues due to faulty neighbor radios
 no Negate a command or set its defaults
 sensitivity Configure smart-rf sensitivity (Modifies various
 other smart-rf configuration items)
 smart-ocs-monitoring Smart off channel scanning

 clrscr Clears the display screen
 commit Commit all changes made in this session
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
```

```
show Show running system information
write Write running configuration to memory or term
```

```
nx9500-6C8809(config-smart-rf-policy-test)#
```

### Related Commands

|                 |                                     |
|-----------------|-------------------------------------|
| <code>no</code> | Removes an existing Smart RF policy |
|-----------------|-------------------------------------|



#### Note

For more information on Smart RF policy commands, see [SMART-RF-POLICY](#).

`t5`

Invokes the configuration mode of a t5 wireless controller

A T5 controller uses the IPX operating system to manage its connected radio devices, as opposed to the WiNG operating system used by RFS controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices.

#### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 7510, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
t5 <T5-DEVICE-MAC>
```

#### Parameters

```
t5 <T5-DEVICE-MAC>
```

|                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>t5 &lt;T5-DEVICE-MAC&gt;</code> | <p>Specify the t5 device's MAC address. The system enters the identified device's configuration mode.</p> <p>A T5 controller uses the IPX operating system to manage its connected radio devices, as opposed to the WiNG operating system used by RFS wireless controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The CPEs (Customer Premises Equipments) are the T5 controller managed radio devices using the IPX operating system. These CPEs use a DSL (Digital Subscriber Line) as their high speed Internet access mechanism using the CPE's physical wallplate connection and phone jack.</p> <p>After logging on to the T5 device, use the 'cpe' keyword and configure the following mandatory settings:</p> <ul style="list-style-type: none"><li>• <code>vlan</code> - Set a VLAN from 1 - 4,094 used as a virtual interface for connections between the T5 controller and its managed CPE devices.</li><li>• <code>start ip</code> - Set a starting IP address used in a range of addresses available to T5 controller connecting CPE devices.</li><li>• <code>end ip</code> - Set an end IP address used in a range of addresses available to T5 controller connecting CPE devices.</li></ul> |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config)#t5 B4:C7:99:ED:5C:2C
nx9500-6C8809(config-device-B4:C7:99:ED:5C:2C)#?
T5 Device Mode commands:
 adsp-sensor-server Configure WIPS server
 bridge Sets MAC address expiration time in the bridge address
 table
 clock Configure clock options
 cpe T5 CPE configuration
 hostname Set system's network name
 interface Select an interface to configure
 ip Internet Protocol (IP)
 no Negate a command or set its defaults
 ntp Configure NTP
 override-wlan Configure RF Domain level overrides for wlan
 password T5 password configuration
 qos QOS settings
 radius-server Radius server settings
 t5 T5 configuration
 t5-logging Modify message logging facilities
 use Set setting to use

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-device-B4:C7:99:ED:5C:2C)#
```

## Related Commands

|                 |                                                                           |
|-----------------|---------------------------------------------------------------------------|
| <code>no</code> | Removes the t5 wireless controller identified by the device's MAC address |
|-----------------|---------------------------------------------------------------------------|

### *web-filter-policy*

Creates a Web Filtering policy and enters its configuration mode. This policy defines rules managing the local classification database and the cached data. When configured and applied, this policy also enables caching of URL classification records in a local database in a controller-based, hierarchically managed (HM) deployment. Use this option to specify the following: classification server details, size of the local database, time for which records are cached in the database, the action taken in case the classification server is unavailable, etc.

The Web filter policy is applied at the profile or device level.

For more information on URL filtering, see [url-filter](#) on page 623.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
web-filter-policy <WEB-FILTER-POLICY-NAME>
```

## Parameters

```
web-filter-policy <WEB-FILTER-POLICY-NAME>
```

|                          |                                                                                  |
|--------------------------|----------------------------------------------------------------------------------|
| <WEB-FILTER-POLICY-NAME> | Specify the Web filter policy name. If the policy does not exist, it is created. |
|--------------------------|----------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config)#web-filter-policy test
nx9500-6C8809(config-web-filter-policy-test)#?
Content Filter Mode commands:
 cache-max-recs Configure the maximum number of records in local cache
 cache-save-interval Configure the time a record is saved in local cache
 logging Select logging method
 no Negate a command or set its defaults
 server-host Configure URL classification server if it is not the
 adopted controller
 server-unreachable Permission to access website when classification server
 is unreachable (default is pass)
 uncategorized-url Permission to website when server fails to classify the
 URL request (default is pass)

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-web-filter-policy-test)#
```

## Related Commands

|    |                                       |
|----|---------------------------------------|
| no | Removes an existing Web filter policy |
|----|---------------------------------------|

## web-filter-config-commands

The following table summarizes Web Filter policy configuration mode commands:

**Table 30: Web Filter Config Mode Commands**

| Command                         | Description                                                                                                                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| cache-max-recs on page 549      | Configures the maximum number of records (URLs and Web pages) cached in the local database                                    |
| cache-save-interval on page 549 | Configures the maximum time period for which a record (URL and Web page classification entry) is cached in the local database |
| logging on page 550             | Configures the method used to log Web filtering events                                                                        |
| server-host on page 550         | Configures the URL classification server in case it is not the adopted controller                                             |



**Table 30: Web Filter Config Mode Commands (continued)**

| Command                                     | Description                                                                                   |
|---------------------------------------------|-----------------------------------------------------------------------------------------------|
| <code>server-unreachable</code> on page 551 | Configures the action taken in case the classification server is unreachable                  |
| <code>uncategorized-url</code> on page 552  | Configures the action taken in case the classification server fails to classify a URL/Website |
| <code>no</code> on page 553                 | Reverts the selected Web Filter policy settings to default                                    |

### cache-max-recs

Configures the maximum number of records (URL and Web page classification entries) cached in the local database

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
cache-max-recs <1-1000000>
```

#### Parameters

```
cache-max-recs <1-1000000>
```

|                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>cache-max-recs &lt;1-1000000&gt;</code> | Specify the maximum number of records cached in the local database from 1 - 1000000.<br>When configuring this value take into consideration the type of device using the Web Filter policy. The value should approximately be as per the following information: <ul style="list-style-type: none"> <li>• NX95XX - &lt;1-1000000&gt; (default is 100000)</li> <li>• NX75XX - &lt;1-100000&gt; (default is 10000)</li> <li>• RFS Switches - &lt;1-10000&gt; (default is 1000)</li> <li>• Access Points - &lt;1-1500&gt; (default is 500)</li> </ul> |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config-web-filter-policy-test)#cache-max-recs 9000
nx9500-6C8809(config-web-filter-policy-test)#show context
web-filter-policy test
 cache-max-recs 9000
nx9500-6C8809(config-web-filter-policy-test)#
```

#### Related Commands

|                             |                                                                                                                                            |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <code>no</code> on page 553 | Reverts the maximum number of stored records to default. Please see the parameter table for default values for the different device types. |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|

### cache-save-interval

Configures the maximum time period, in seconds, for which a record (URL and Web page classification entry) is cached in the local database. Once the specified time has expired the record is removed from the cache.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
cache-save-interval <1-86400>
```

#### Parameters

```
cache-save-interval <1-86400>
```

|                               |                                                                                                                                                    |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| cache-save-interval <1-86400> | Specify the maximum time period, in seconds, for which a record is cached in the local database from 1 - 86400 seconds. The default is 60 seconds. |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config-web-filter-policy-test)#cache-save-interval 1000
nx9500-6C8809(config-web-filter-policy-test)#show context
web-filter-policy test
 cache-max-recs 9000
 cache-save-interval 1000
nx9500-6C8809(config-web-filter-policy-test)#
```

#### Related Commands

|                       |                                                                                                                                            |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>no</b> on page 553 | Reverts the maximum time period for which a record (URL and Web page classification entry) is cached in the local database to default (60) |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------|

## logging

Configures the method used to log Web filtering events

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
logging [logfile|syslog]
```

#### Parameters

```
logging [logfile|syslog]
```

|                          |                                                                                                                                                                                                                              |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| logging [logfile syslog] | Selects the method used to log Web filtering events. The options are: <ul style="list-style-type: none"><li>• logfile - Logs to a file.</li><li>• syslog - Logs to the syslog server. This is the default setting.</li></ul> |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config-web-filter-policy-test)#logging logfile
nx9500-6C8809(config-web-filter-policy-test)#show context
web-filter-policy test
 logging logfile
nx9500-6C8809(config-web-filter-policy-test)#
```

## server-host

Configures the URL classification server in case it is not the adopted controller

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
server-host [host-name <SERVER-HOST-NAME>|ip-address <SERVER-IPv4>|mint-id <SERVER-MiNT-ID>]
```

#### Parameters

```
server-host [host-name <SERVER-HOST-NAME>|ip-address <SERVER-IPv4>|mint-id <SERVER-MiNT-ID>]
```

|                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| server-host [host-name <SERVER-HOST-NAME> ip-address <SERVER-IPv4> mint-id <SERVER-MiNT-ID>] | Use one of the following options to identify the URL classification server: <ul style="list-style-type: none"><li>• host-name &lt;SERVER-HOST-NAME&gt; - Identifies the classification server by its hostname.</li><li>• ip-address &lt;SERVER-IPv4&gt; - Identifies the classification server by its IP address.</li><li>• mint-id &lt;SERVER-MiNT-ID&gt; - Identifies the classification server by its MiNT ID.</li></ul> |
|----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config-web-filter-policy-test)#server-host ip-address 192.168.13.13
nx9500-6C8809(config-web-filter-policy-test)#show context
web-filter-policy test
 cache-max-recs 9000
 cache-save-interval 1000
 server-host ip-address 192.168.13.13
nx9500-6C8809(config-web-filter-policy-test)#
```

#### Related Commands

|                                |                                                                                                       |
|--------------------------------|-------------------------------------------------------------------------------------------------------|
| <a href="#">no</a> on page 553 | Removes the URL classification server's configured details, such as hostname, ip-address, or MiNT ID. |
|--------------------------------|-------------------------------------------------------------------------------------------------------|

### server-unreachable

Configures the action taken in case the classification server is unreachable. Based on the value configured the an end user's request for a URL/Website is either blocked or passed.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
server-unreachable [block|pass]
```

#### Parameters

```
server-unreachable [block|pass]
```

|                                    |                                                                                                                                                                                                                                                                                                |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| server-unreachable<br>[block pass] | Configures the action taken in case the classification server is unreachable. The options are: <ul style="list-style-type: none"> <li>• block - Denies access to the requested URL/Website</li> <li>• pass - Allows access to the requested URL/Website. This is the default value.</li> </ul> |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```

nx9500-6C8809(config-web-filter-policy-test)#server-unreachable block
nx9500-6C8809(config-web-filter-policy-test)#show context
web-filter-policy test
 cache-max-recs 9000
 cache-save-interval 1000
 server-unreachable block
 server-host ip-address 192.168.13.13
nx9500-6C8809(config-web-filter-policy-test)#

```

### Related Commands

|                |                                                                                             |
|----------------|---------------------------------------------------------------------------------------------|
| no on page 553 | Reverts the action taken in case the classification server is unreachable to default (pass) |
|----------------|---------------------------------------------------------------------------------------------|

## uncategorized-url

Configures the action taken in case the classification server fails to classify a URL/Website. Based on the value configured the an end user's request for a non-classified URL/Website is either blocked or passed.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
uncategorized-url [block|pass]
```

### Parameters

```
uncategorized-url [block|pass]
```

|                                |                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| uncategorized-url [block pass] | Configures the action taken in case the classification server fails to classify a URL/Website. The options are: <ul style="list-style-type: none"> <li>• block - Denies access to the requested non-classified URL/Website</li> <li>• pass - Allows access to the requested non-classified URL/Website. This is the default value.</li> </ul> |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```

nx9500-6C8809(config-web-filter-policy-test)#uncategorized-url block
nx9500-6C8809(config-web-filter-policy-test)#show context
web-filter-policy test
 cache-max-recs 9000
 cache-save-interval 1000
 uncategorized-url block
 server-unreachable block
 server-host ip-address 192.168.13.13
nx9500-6C8809(config-web-filter-policy-test)#

```

### Related Commands

no on page 553

no

Reverts the selected Web Filter policy settings to default, based on the parameters passed

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
no [cache-max-recs|cache-save-interval|server-host|server-unreachable|uncategorized-url]
```

Parameters

```
no <PARAMETERS>
```

|                 |                                                                                                                                                     |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| no <PARAMETERS> | Reverts the selected Web Filter policy settings to default, based on the parameters passed. Specify the parameters to revert back to default value. |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|

Examples

The following example shows the Web Filter policy 'test' settings before the 'no' command is executed:

```
nx9500-6C8809(config-web-filter-policy-test)#show context
web-filter-policy test
 cache-max-recs 9000
 cache-save-interval 1000
 uncategorized-url block
 server-unreachable block
 server-host ip-address 192.168.13.13
nx9500-6C8809(config-web-filter-policy-test)#
nx9500-6C8809(config-web-filter-policy-test)#no cache-max-recs
nx9500-6C8809(config-web-filter-policy-test)#no server-unreachable
nx9500-6C8809(config-web-filter-policy-test)#no uncategorized-url
```

The following example shows the Web Filter policy 'test' settings after the 'no' command has been executed:

```
nx9500-6C8809(config-web-filter-policy-test)#show context
web-filter-policy test
 cache-save-interval 1000
 server-host ip-address 192.168.13.13
nx9500-6C8809(config-web-filter-policy-test)#
```

*wips-policy*

Configures a WIPS policy and enters its configuration mode

**Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
wips-policy <WIPS-POLICY-NAME>
```

## Parameters

```
wips-policy <WIPS-POLICY-NAME>
```

<WIPS-POLICY-NAME> Specify the WIPS policy name. If A policy with the specified name does not exist, it is created.

## Examples

```
nx9500-6C8809(config)#wips-policy test
nx9500-6C8809(config-wips-policy-test)#?
Wips Policy Mode commands:
 ap-detection Rogue AP detection
 enable Enable this wips policy
 event Configure an event
 history-throttle-duration Configure the duration for which event duplicates
 are not stored in history
 interference-event Specify events which will contribute to smart-rf
 wifi interference calculations
 no Negate a command or set its defaults
 signature Signature to configure
 use Set setting to use

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-wips-policy-test)#
```

## Related Commands

**no** Removes an existing WIPS policy



### Note

For more information on WIPS Policy commands, see [WIPS-POLICY](#).

## wlan

Configures a WLAN and enters its configuration mode. Use this command to modify an existing WLAN's settings.

A WLAN is a data-communications system that flexibly extends the functionality of a wired LAN. A WLAN links two or more computers or devices using spread-spectrum or OFDM (Orthogonal Frequency Division Multiplexing) modulation based technology. WLANs do not require lining up devices for line-of-sight transmission, and are thus, desirable for wireless networking. Roaming users can be handed off from one access point to another, like a cellular phone system. WLANs can therefore be configured around the needs of specific user groups, even when they are not in physical proximity.

WLANs can provide an abundance of services, including data communications (allowing mobile devices to access applications), e-mail, file, and print services or even specialty applications (such as guest access control and asset tracking).

Each WLAN configuration contains encryption, authentication and QoS policies and conditions for user connections. Connected Access Point radios transmit periodic beacons for each BSS. A beacon advertises the SSID, security requirements, supported data rates of the wireless network to enable clients to locate and connect to the WLAN.

WLANs are mapped to radios on each Access Point. A WLAN can be advertised from a single Access Point radio or can span multiple Access Points and radios. WLAN configurations can be defined to provide service to specific areas of a site. For example, a guest access WLAN may only be mapped to a 2.4 GHz radio in a lobby or conference room providing limited coverage, while a data WLAN is mapped to all 2.4 GHz and 5.0 GHz radios at the branch site to provide complete coverage.

The maximum number of WLANs supported by different devices is as follows:

- RFS 4000 controllers support a maximum of 32 WLANs. An Access Point supports a maximum of 16 WLANs.
- NX9XXX series service platforms – 1000 WLANs
- Access Points – 16 WLANs

**Supported in the following platforms:**

- Access Points – AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers – RFS 4000
- Service Platforms – NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

**Syntax**

```
wlan {<WLAN-NAME>|containing <WLAN-NAME>}
```

**Parameters**

```
wlan {<WLAN-NAME>|containing <WLAN-NAME>}
```

|                        |                                                                                                                                                                                                                                                                                                          |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wlan <WLAN-NAME>       | Configures a new WLAN <ul style="list-style-type: none"> <li>• &lt;WLAN-NAME&gt; - Optional. Specify the WLAN name.</li> </ul> <p><b>Note:</b> The WLAN name could be a logical representation of its coverage area (for example, engineering, marketing etc.).The name cannot exceed 32 characters.</p> |
| containing <WLAN-NAME> | Optional. Configures an existing WLAN's settings <ul style="list-style-type: none"> <li>• &lt;WLAN-NAME&gt; – Specify a sub-string in the WLAN name. Use this parameter to filter a WLAN. This option allows you to select and enter the configuration mode of one or more WLANs.</li> </ul>             |

**Examples**

```
nx9500-6C8809(config)#wlan wlan1
nx9500-6C8809(config-wlan-wlan1)#?
```

Wireless LAN Mode commands:

```
accounting
```

Configure how accounting records are created for this wlan

```
acl
```

Actions taken based on ACL

|                                       |                                                                                    |
|---------------------------------------|------------------------------------------------------------------------------------|
|                                       | configuration [ packet drop being one of them]                                     |
| answer-broadcast-probes               | Include this wlan when responding to probe requests that do not specify an SSID    |
| assoc-response                        | Association response threshold                                                     |
| association-list                      | Configure the association list for the wlan                                        |
| authentication-type                   | The authentication type of this WLAN                                               |
| bridging-mode                         | Configure how packets to/from this wlan are bridged                                |
| broadcast-dhcp                        | Configure broadcast DHCP packet handling                                           |
| broadcast-ssid                        | Advertise the SSID of the WLAN in beacons                                          |
| captive-portal-enforcement            | Enable captive-portal enforcement on the wlan                                      |
| client-access                         | Enable client-access (normal data operations) on this wlan                         |
| client-client-communication           | Allow switching of frames from one wireless client to another on this wlan         |
| client-load-balancing                 | Configure load balancing of clients on this wlan                                   |
| controller-assisted-mobility          | Enable controller assisted mobility to determine wireless clients' VLAN assignment |
| data-rates                            | Specify the 802.11 rates to be supported on this wlan                              |
| description                           | Configure a description of the usage of this wlan                                  |
| downstream-group-addressed-forwarding | Enable downstream group addressed forwarding of packets                            |
| dpi                                   | Deep-Packet-Inspection (Application Assurance)                                     |
| dynamic-vlan-assignment               | Dynamic VLAN assignment configuration                                              |
| eap-types                             | Configure client access based on eap-type used for authentication                  |
| encryption-type                       | Configure the encryption to use on this wlan                                       |
| enforce-dhcp                          | Drop packets from Wireless Clients with static IP address                          |
| fast-bss-transition                   | Configure support for 802.11r Fast BSS Transition                                  |
| http-analyze                          | Enable HTTP URL analysis on the wlan                                               |
| ip                                    | Internet Protocol (IP)                                                             |
| ipv6                                  | Internet Protocol version 6 (IPv6)                                                 |
| kerberos                              | Configure kerberos authentication parameters                                       |
| mac-authentication                    | Configure mac-authentication related parameters                                    |
| no                                    | Negate a command or set its defaults                                               |
| nsight                                | Nsight Server                                                                      |
| opendns                               | OpenDNS related config for this wlan                                               |
| protected-mgmt-frames                 | Protected Management Frames (IEEE 802.11w) related configuration                   |
| proxy-arp-mode                        | Configure handling of ARP requests with proxy-arp is enabled                       |
| proxy-nd-mode                         | Configure handling of IPv6 ND requests with proxy-nd is enabled                    |
| qos-map                               | Support the 802.11u QoS map element and frame                                      |
| radio-resource-measurement            | Configure support for 802.11k Radio Resource Measurement                           |



|                     |                                                                                                                             |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------|
| radius              | Configure RADIUS related parameters                                                                                         |
| registration        | Enable dynamic registration of device (or) user                                                                             |
| relay-agent         | Configure dhcp relay agent info                                                                                             |
| shutdown            | Shutdown this wlan                                                                                                          |
| ssid                | Configure the Service Set Identifier for this WLAN                                                                          |
| t5-client-isolation | Isolate traffic among clients                                                                                               |
| t5-security         | Configure encryption and authentication                                                                                     |
| time-based-access   | Configure client access based on time                                                                                       |
| use                 | Set setting to use                                                                                                          |
| vlan                | Configure the vlan where traffic from this wlan is mapped                                                                   |
| vlan-pool-member    | Add a member vlan to the pool of vlans for the wlan (Note: configuration of a vlan-pool overrides the 'vlan' configuration) |
| wep128              | Configure WEP128 parameters                                                                                                 |
| wep64               | Configure WEP64 parameters                                                                                                  |
| wing-extensions     | Enable support for WiNG-Specific extensions to 802.11                                                                       |
| wireless-client     | Configure wireless-client specific parameters                                                                               |
| wpa-wpa2            | Modify tkip-ccmp (wpa/wpa2) related parameters                                                                              |
| clrscr              | Clears the display screen                                                                                                   |
| commit              | Commit all changes made in this session                                                                                     |
| do                  | Run commands from Exec mode                                                                                                 |
| end                 | End current mode and change to EXEC mode                                                                                    |
| exit                | End current mode and down to previous mode                                                                                  |
| help                | Description of the interactive help system                                                                                  |
| revert              | Revert changes                                                                                                              |
| service             | Service Commands                                                                                                            |
| show                | Show running system information                                                                                             |
| write               | Write running configuration to memory or terminal                                                                           |

```
nx9500-6C8809(config-wlan-wlan1)#
```

The following example shows how to use the 'containing' keyword to enter the configuration mode of an existing WLAN:

```
nx9500-6C8809(config)#wlan containing wlan1
nx9500-6C8809(config-wlan-{'containing': 'wlan1'})#
```

### Related Commands

|           |                                          |
|-----------|------------------------------------------|
| <b>no</b> | Removes an existing WLAN from the system |
|-----------|------------------------------------------|

### wlan-config-mode-commands

This section documents the WLAN configuration mode commands in detail.

Use the (config) instance to configure WLAN related parameters.

To navigate to this instance, use the following command:

```
<DEVICE> (config)#wlan <WLAN-NAME>
```

The following table lists the WLAN configuration mode commands:

Table: WLAN Config Mode Commands

| Command                                               | Description                                                                                                                                           |
|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">accounting</a>                            | Defines a WLAN's accounting settings                                                                                                                  |
| <a href="#">acl</a>                                   | Defines the actions based on an ACL rule configuration                                                                                                |
| <a href="#">answer-broadcast-probes</a>               | Allows a WLAN to respond to probes for broadcast ESS                                                                                                  |
| <a href="#">assoc-response</a> on page 562            | Configures a minimum RSSI (receive signal strength indication) value, below which the WLAN does not send a response to a client's association request |
| <a href="#">association-list</a>                      | Attaches an existing global association list to a WLAN                                                                                                |
| <a href="#">authentication-type</a>                   | Sets a WLAN's authentication type                                                                                                                     |
| <a href="#">bridging-mode</a>                         | Configures how packets are bridged to/from this WLAN                                                                                                  |
| <a href="#">broadcast-dhcp</a>                        | Configures broadcast DHCP packet handling                                                                                                             |
| <a href="#">broadcast-ssid</a>                        | Advertises a WLAN's SSID in beacons                                                                                                                   |
| <a href="#">captive-portal-enforcement</a>            | Configures a WLAN's captive portal enforcement                                                                                                        |
| <a href="#">client-access</a>                         | Enables WLAN client access (normal data operations)                                                                                                   |
| <a href="#">client-client-communication</a>           | Allows the switching of frames from one wireless client to another on a WLAN                                                                          |
| <a href="#">client-load-balancing</a>                 | Enables load balancing of WLAN clients                                                                                                                |
| <a href="#">controller-assisted-mobility</a>          | Enables controller assisted mobility to determine wireless clients' VLAN assignment                                                                   |
| <a href="#">data-rates</a>                            | Specifies the 802.11 rates supported on the WLAN                                                                                                      |
| <a href="#">description</a>                           | Sets a WLAN's description                                                                                                                             |
| <a href="#">downstream-group-addressed-forwarding</a> | Enables forwarding of downstream packets addressed to a group                                                                                         |
| <a href="#">dynamic-vlan-assignment</a>               | Configures dynamic VLAN assignment on this WLAN                                                                                                       |
| <a href="#">eap-types</a>                             | Configures client access based on eap-type used for authentication                                                                                    |
| <a href="#">encryption-type</a>                       | Sets a WLAN's encryption type                                                                                                                         |
| <a href="#">enforce-dhcp</a>                          | Drops packets from clients with a static IP address                                                                                                   |
| <a href="#">fast-bss-transition</a>                   | Configures support for 802.11r fast BSS transition on a WLAN                                                                                          |
| <a href="#">http-analyze</a>                          | Enables HTTP URL analysis on the WLAN                                                                                                                 |
| <a href="#">ip</a>                                    | Configures IP settings                                                                                                                                |
| <a href="#">kerberos</a>                              | Configures Kerberos authentication parameters                                                                                                         |
| <a href="#">mac-authentication</a>                    | Configures MAC authentication parameters                                                                                                              |
| <a href="#">no (wlan-config-mode)</a> on page 619     | Negates a command or reverts settings to their default                                                                                                |
| <a href="#">proxy-arp-mode</a> on page 588            | Enables the proxy ARP mode for ARP requests                                                                                                           |

| Command                                  | Description                                                                       |
|------------------------------------------|-----------------------------------------------------------------------------------|
| <code>radio-resource-measurement</code>  | Enables support for 802.11k radio resource measurement                            |
| <code>radius</code>                      | Configures RADIUS parameters                                                      |
| <code>relay-agent</code>                 | Enables support for DHCP relay agent information (option 82) feature on this WLAN |
| <code>shutdown</code>                    | Shuts down a WLAN                                                                 |
| <code>ssid</code>                        | Configures a WLAN's SSID                                                          |
| <code>time-based-access</code>           | Configures time-based client access                                               |
| <code>use</code>                         | Defines WLAN mode configuration settings                                          |
| <code>vlan</code>                        | Assigns a VLAN for the WLAN                                                       |
| <code>vlan-pool-member</code>            | Adds a member VLAN to the pool of VLANs for a WLAN                                |
| <code>wep128</code>                      | Configures WEP128 parameters                                                      |
| <code>wep64</code>                       | Configures WEP64 parameters                                                       |
| <code>wing-extensions</code> on page 613 | Enables support for WiNG specific extensions to 802.11                            |
| <code>wireless-client</code>             | Configures the transmit power for wireless clients transmission                   |
| <code>wpa-wpa2</code>                    | Modifies TKIP and CCMP (WPA/WPA2) related parameters                              |
| <code>service</code>                     | Invokes service commands applicable in the WLAN configuration mode                |

#### accounting (wlan-config-mode)

Defines the WLAN's accounting configuration

Accounting is the method of collecting user data, such as start and stop times, executed commands (for example, PPP), number of packets and number of bytes received and transmitted. This data is sent to the security server for billing, auditing, and reporting purposes. Accounting enables wireless network administrators to track the services and network resources accessed and consumed by users. When enabled, this feature allows the network access server to report and log user activity to a RADIUS security server in the form of accounting records. Each accounting record is comprised of AV pairs and is stored on the access control server. The data can be analyzed for network management, client billing, and/or auditing. Accounting methods must be defined through AAA policies.

Accounting can be enabled and applied to Access Point, wireless controller, or service platform managed WLANs. Once enabled, it uniquely logs accounting events specific to the managed WLAN. Accounting logs contain information about the use of remote access services by users. This information is of great assistance in partitioning local versus remote users and how to best accommodate each. Remote user information can be archived to a location outside of the Access Point for periodic network and user permission administration.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
accounting [radius|syslog|wait-client-ip]
accounting [radius|wait-client-ip]
accounting syslog [host|mac-address-format]
accounting syslog host <IP/HOSTNAME> {port <1-65535>}
{proxy-mode [none|through-controller|through-rf-domain-manager]}
accounting syslog mac-address-format [middle-hyphen|no-delim|pair-colon|
pair-hyphen|quad-dot] case [lower|upper]
```

## Parameters

```
accounting [radius|wait-client-ip]
```

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| accounting radius         | Enables support for WLAN RADIUS accounting messages. This option is disabled by default. When enabled, the WLAN uses an external RADIUS resource for accounting. Use the <b>use &gt; aaa-policy &gt; &lt;AAA-POLICY-NAME&gt;</b> command to associate an appropriate AAA policy with this WLAN. This AAA policy should be existing and should define the accounting, authentication, and authorization parameters. |
| accounting wait-client-ip | Enables waiting for client's IP before commencing the accounting procedure                                                                                                                                                                                                                                                                                                                                         |

```
accounting syslog host <IP/HOSTNAME> {port <1-65535>}
{proxy-mode [none|through-controller|through-rf-domain-manager]}
```

|                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| accounting syslog                                                  | Enables support for WLAN syslog accounting messages in standard syslog format (RFC 3164). This option is disabled by default.                                                                                                                                                                                                                                                                                    |
| host <IP/HOSTNAME>                                                 | Configures a syslog destination hostname or IP address for accounting records <ul style="list-style-type: none"> <li>&lt;IP/HOSTNAME&gt; - Specify the IP address or name of the destination host.</li> </ul>                                                                                                                                                                                                    |
| port <1-65535>                                                     | Optional. Configures the syslog server's UDP port (this port is used to connect to the server) <ul style="list-style-type: none"> <li>&lt;1-65535&gt; - Specify the port from 1 - 65535. Default port is 514.</li> </ul>                                                                                                                                                                                         |
| proxy-mode [none]<br>through-controller through-rf-domain-manager] | Optional. Configures the request proxying mode <ul style="list-style-type: none"> <li>none - Requests are directly sent to the server from the device</li> <li>through-controller - Proxies requests through the controller (Access Point, wireless controller, or service platform) configuring the device</li> <li>through-rf-domain-manager - Proxies requests through the local RF Domain manager</li> </ul> |

```
accounting syslog mac-address-format [middle-hyphen|no-delim|pair-colon|pair-hyphen|
quad-dot] case [lower|upper]
```

|                    |                                                                                                                 |
|--------------------|-----------------------------------------------------------------------------------------------------------------|
| accounting syslog  | Enables support for WLAN syslog accounting messages                                                             |
| mac-address-format | Configures the MAC address format used in syslog messages                                                       |
| middle-hyphen      | Configures the MAC address format with middle hyphen (AABBCC-DDEEFF)                                            |
| no-delim           | Configures the MAC address format without delimiters (AABBCCDDEEFF)                                             |
| pair-colon         | Configures the MAC address format with pair-colon delimiters (AA:BB:CC:DD:EE:FF)                                |
| pair-hyphen        | Configures the MAC address format with pair-hyphen delimiters (AA-BB-CC-DD-EE-FF). This is the default setting. |

|                    |                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| quad-dot           | Configures the MAC address format with quad-dot delimiters (AABB.CCDD.EEFF)                                                                                                                                                                                                                                                                                                                    |
| case [lower upper] | The following keywords are common to all: <ul style="list-style-type: none"> <li>• case – Specifies MAC address case (upper or lower) <ul style="list-style-type: none"> <li>• lower – Specifies MAC address is filled in lower case (for example, aa-bb-cc-dd-ee-ff)</li> <li>• upper – Specifies MAC address is filled in upper case (for example, AA-BB-CC-DD-EE-FF)</li> </ul> </li> </ul> |

### Examples

```

nx9500-6C8809(config-wlan-test)#accounting syslog host 172.16.10.4 port 2 proxy-mode none
nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
accounting syslog host 172.16.10.4 port 2
nx9500-6C8809(config-wlan-test)#

```

### Related Commands

|    |                                                                                                                                                                 |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| no | Disables sending of accounting message to the RADIUS server, disables syslog accounting, or disables waiting for client's IP before sending accounting messages |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|

## acl

Defines the actions taken based on an ACL rule configuration

Use the **use > ip-access-list <IP-ACCESS-LIST-NAME>** command to associate an ACL with the WLAN. The ACL rule is determined by the associated ACL's configuration.

A firewall is a mechanism enforcing access control, and is considered a first line of defense in protecting proprietary information within the network. The means by which this is accomplished varies, but in principle, a Firewall can be thought of as mechanisms allowing and denying data traffic in respect to administrator defined rules.

WLANs use firewalls like ACLs (Access Control Lists) to filter/mark packets based on the WLAN from which they arrive, as opposed to filtering packets on layer 2 ports. An ACL contains an ordered list of ACEs (Access Control Entries). Each ACE specifies an action and a set of conditions (rules) a packet must satisfy to match the ACE. The order of conditions in the list is critical since filtering is stopped after the first match.

IP based Firewall rules are specific to source and destination IP addresses and the unique rules and precedence orders assigned. Both IP and non-IP traffic on the same layer 2 interface can be filtered by applying both an IP ACL and a MAC.

Additionally, you can filter layer 2 traffic on a physical layer 2 interface using MAC addresses. A MAC Firewall rule uses source and destination MAC addresses for matching operations, where the result is a typical allow, deny or mark designation to WLAN packet traffic.

Keep in mind IP and non-IP traffic on the same layer 2 interface can be filtered by applying both an IP ACL and a MAC ACL to the interface.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
acl exceed-rate wireless-client-denied-traffic <0-1000000> {blacklist <0-86400>|
disassociate}
```

### Parameters

```
acl exceed-rate wireless-client-denied-traffic <0-1000000> {blacklist <0-86400>|
disassociate}
```

|                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| acl exceed-rate                            | Sets the actions taken based on an ACL rule configuration (for example, drop a packet) <ul style="list-style-type: none"> <li>• exceed-rate - Action is taken when the rate exceeds a specified value</li> </ul>                                                                                                                                                                                                                                                                      |
| wireless-client-denied-traffic <0-1000000> | Sets the action to deny traffic to the wireless client when the rate exceeds the specified value <ul style="list-style-type: none"> <li>• &lt;0-1000000&gt; - Specify a allowed rate threshold of disallowed traffic in packets/sec.</li> </ul> <p>If enabled, this option allows an associated client, exceeding the thresholds configured for storm traffic, to be either de-authenticated or blacklisted depending on the action selected. This option is disabled by default.</p> |
| blacklist <0-86400>                        | Optional. Sets the time period for which an offending wireless client is blacklisted. <ul style="list-style-type: none"> <li>• &lt;0-86400&gt; - Configures the blacklist duration from 0 - 86400 seconds. Offending clients are re-authenticated once the blacklist duration, configured here, is over.</li> </ul>                                                                                                                                                                   |
| disassociate                               | Optional. When enabled, disassociates a blacklisted wireless client.                                                                                                                                                                                                                                                                                                                                                                                                                  |

### Examples

```
nx9500-6C8809(config-wlan-test)#acl exceed-rate wireless-client-denied-traffic
20 disassociate
nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 accounting syslog host 172.16.10.4 port 2
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
nx9500-6C8809(config-wlan-test)#
```

### Related Commands

|    |                                                                                                                                             |
|----|---------------------------------------------------------------------------------------------------------------------------------------------|
| no | Removes the action (de-authenticate or blacklist) to be taken when an associated client exceeds the thresholds configured for storm traffic |
|----|---------------------------------------------------------------------------------------------------------------------------------------------|

### assoc-response

Configures the deny-threshold and rssi-threshold values. These threshold values are considered when responding to a client's association/authentication request.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
assoc-response [deny-threshold <1-12>|rssi-threshold <-100--40>]
```

#### Parameters

```
assoc-response [deny-threshold <1-12>|rssi-threshold <-100--40>]
```

|                           |                                                                                                                                                                                                                                                                                                                                          |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| assoc-response            | Configures the association response thresholds                                                                                                                                                                                                                                                                                           |
| deny-threshold <1-12>     | Configures the number of times association/authentication request, from a client, is ignored if the RSSI is less than the configured RSSI threshold. This option is disabled by default. <ul style="list-style-type: none"> <li>• &lt;1-12&gt; - Specify the deny-threshold from 1 - 12.</li> </ul>                                      |
| rssi-threshold <-100--40> | Configures an association response RSSI threshold value. If the RSSI is below the configured threshold value, the client's association/authentication request is ignored. This option is disabled by default. rssi-threshold <ul style="list-style-type: none"> <li>• &lt;-100--40&gt; - Specify a value from -100 - -40 dBm.</li> </ul> |

#### Examples

```
nx9500-6C8809(config-wlan-test)#assoc-response rssi-threshold -60
nx9500-6C8809(config-wlan-test)#assoc-response deny-threshold 4
nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type none
 assoc-response rssi-threshold -60
 assoc-response deny-threshold 4
 registration user group-name guest expiry-time 2000 agreement-refresh 14400
nx9500-6C8809(config-wlan-test)#
```

#### Related Commands

|           |                                                                 |
|-----------|-----------------------------------------------------------------|
| <b>no</b> | Removes the configured deny-threshold and rssi-threshold values |
|-----------|-----------------------------------------------------------------|

#### answer-broadcast-probes

Allows the WLAN to respond to probe requests that do not specify an SSID. These probes are for broadcast ESS. This feature is enabled by default.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
answer-broadcast-probes
```

#### Parameters

None

## Examples

```
nx9500-6C8809(config-wlan-1)#answer-broadcast-probes
nx9500-6C8809(config-wlan-1)#
```

## Related Commands

|                 |                                                                                  |
|-----------------|----------------------------------------------------------------------------------|
| <code>no</code> | Does not allow this WLAN to respond to probe requests that do not specify a SSID |
|-----------------|----------------------------------------------------------------------------------|

## association-list

Attaches an existing global association list with this WLAN. For more information on global association lists, see [global-association-list](#).

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
association-list global <GLOBAL-ASSO-LIST-NAME>
```

## Parameters

```
association-list global <GLOBAL-ASSO-LIST-NAME>
```

|                                                                    |                                                                                                                                                                                                                                          |
|--------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>association-list global &lt;GLOBAL-ASSO-LIST-NAME&gt;</code> | Attaches an existing global association list with this WLAN <ul style="list-style-type: none"><li>• <code>&lt;GLOBAL-ASSO-LIST-NAME&gt;</code> - Specify the global association list name (should be existing and configured).</li></ul> |
|--------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
rfs4000-1B3596(config-wlan-test)#association-list global my-clients
rfs4000-1B3596(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 association-list global my-clients
rfs4000-1B3596(config-wlan-test)#
```

## Related Commands

|                 |                                                                  |
|-----------------|------------------------------------------------------------------|
| <code>no</code> | Removes the global association list's association with this WLAN |
|-----------------|------------------------------------------------------------------|

## authentication-type

Sets the WLAN's authentication type

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
authentication-type [eap|eap-mac|eap-psk|kerberos|mac|none]
```



## Parameters

`authentication-type [ eap | eap-mac | eap-psk | kerberos | mac | none ]`

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| authentication-type | Configures a WLAN's authentication type<br>The authentication types are: EAP, EAP-MAC, EAP-PSK, Kerberos, MAC, and none.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| eap                 | Configures EAP authentication (802.1X)<br>EAP is the de-facto standard authentication method used to provide secure authenticated access to controller managed WLANs. EAP provides mutual authentication, secured credential exchange, dynamic keying and strong encryption. 802.1X EAP can be deployed with WEP, WPA or WPA2 encryption schemes to further protect user information forwarded over controller managed WLANs.<br>The EAP process begins when an unauthenticated supplicant (client device) tries to connect with an authenticator (in this case, the authentication server). An Access Point passes EAP packets from the client to an authentication server on the wired side of the Access Point. All other packet types are blocked until the authentication server (typically, a RADIUS server) verifies the client's identity.<br>If using EAP authentication ensure that a AAA policy is mapped to the WLAN. |
| eap-mac             | Configures EAP or MAC authentication depending on client. (This setting is valid only with the None encryption type).<br>EAP-MAC is useful when in a hotspot environment, as some clients support EAP and an administrator may want to authenticate based on just the MAC address of the device.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| eap-psk             | Configures EAP authentication or pre-shared keys depending on client (This setting is only valid with TKIP (Temporal Key Integrity Protocol) or CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) encryption types).<br>When using PSK with EAP, the controller sends a packet requesting a secure link using a pre-shared key. The controller and authenticating device must use the same authenticating algorithm and passcode during authentication. EAP-PSK is useful when transitioning from a PSK network to one that supports EAP.<br>If using eap-psk authentication ensure that a AAA policy is mapped to the WLAN.                                                                                                                                                                                                                                                                    |
| kerberos            | Configures Kerberos authentication (encryption will change to WEP128 if it's not already WEP128 or Keyguard)<br>Kerberos (designed and developed by MIT) provides strong authentication for client/server applications using secret-key cryptography. Using Kerberos, a client must prove its identity to a server (and vice versa) across an insecure network connection.<br>Once a client and server use Kerberos to validate their identity, they encrypt all communications to assure privacy and data integrity. Kerberos can only be used on the access point with 802.11b clients. Kerberos uses NTP (Network Time Protocol) for synchronizing the clocks of its KDC (Key Distribution Center ) server(s).                                                                                                                                                                                                                 |
| mac                 | Configures MAC authentication (RADIUS lookup of MAC address)<br>MAC is a device level authentication method used to augment other security schemes when legacy devices are deployed using static WEP.<br>MAC authentication can be used for device level authentication by permitting WLAN access based on device MAC address. MAC authentication is typically used to augment WLAN security options that do not use authentication (such as static WEP, WPA-PSK and WPA2-PSK) MAC authentication can also be used to assign VLAN memberships, firewall policies and time and date restrictions.<br>MAC authentication can only identify devices, not users.<br>If using mac authentication ensure that an AAA policy is mapped to the WLAN.                                                                                                                                                                                      |
| none                | No authentication is used or the client uses pre-shared keys                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## Examples

```
nx9500-6C8809(config-wlan-test)#authentication-type eap
nx9500-6C8809(config-wlan-test)#show context
wlan test
ssid test
```

```

bridging-mode tunnel
encryption-type none
authentication-type eap
accounting syslog host 172.16.10.4 port 2
acl exceed-rate wireless-client-denied-traffic 20 disassociate
nx9500-6C8809(config-wlan-test)#

```

#### Related Commands

|           |                                                                                      |
|-----------|--------------------------------------------------------------------------------------|
| <b>no</b> | Resets the authentication mode used with this WLAN to default (none/pre-shared keys) |
|-----------|--------------------------------------------------------------------------------------|

### bridging-mode

Configures the mode used to bridge packets to and from a WLAN

Use this command to define which VLANs are bridged, and how local VLANs are bridged between the wired and wireless sides of the network.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
bridging-mode [local|tunnel]
```

#### Parameters

```
bridging-mode [local|tunnel]
```

|               |                                                                                        |
|---------------|----------------------------------------------------------------------------------------|
| bridging-mode | Configures bridging mode on this WLAN. The options are local and tunnel.               |
| local         | Bridges packets between WLAN and local ethernet ports. This is the default mode.       |
| tunnel        | Tunnels packets to other devices (typically a wireless controller or service platform) |

#### Examples

```

nx9500-6C8809(config-wlan-test)#bridging-mode local
nx9500-6C8809(config-wlan-test)#show context
wlan test
ssid test
bridging-mode local
encryption-type none
authentication-type eap
accounting syslog host 172.16.10.4 port 2
acl exceed-rate wireless-client-denied-traffic 20 disassociate
nx9500-6C8809(config-wlan-test)#

```

### broadcast-dhcp

Configures broadcast DHCP packet handling parameters

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
broadcast-dhcp validate-offer
```

### Parameters

```
broadcast-dhcp validate-offer
```

`validate-offer` Enables validation of the broadcast DHCP packet destination (a wireless client associated to the radio) before forwarding over the air. This option is disabled by default.

### Examples

```
nx9500-6C8809(config-wlan-test)#broadcast-dhcp validate-offer
nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type eap
 accounting syslog host 172.16.10.4 port 2
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
broadcast-dhcp validate-offer
nx9500-6C8809(config-wlan-test)#
```

### Related Commands

`no` Disables validation of the broadcast DHCP packet destination (a wireless client associated to the radio) before forwarding over the air

## broadcast-ssid

Advertises the WLAN SSID in beacons. If a hacker tries to isolate and hack a SSID from a client, the SSID will display since the ESSID is in the beacon. This feature is enabled by default.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
broadcast-ssid
```

### Parameters

None

### Examples

```
nx9500-6C8809(config-wlan-1)#broadcast-ssid
nx9500-6C8809(config-wlan-1)#
```

### Related Commands

`no` Disables the broadcasting of the WLAN's SSID in beacons

## captive-portal-enforcement

Configures the captive portal enforcement on this WLAN. When enabled, provides successfully authenticated guests temporary and restricted access to the network. If enforcing captive-portal authentication, associate captive-portal policy with the WLAN. For more information, see [use](#).

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

`captive-portal-enforcement {fall-back}`

#### Parameters

`captive-portal-enforcement {fall-back}`

|                                         |                                                                                                                          |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <code>captive-portal-enforcement</code> | Enables captive portal enforcement on a WLAN. This option is disabled by default.                                        |
| <code>fall-back</code>                  | Optional. Enforces captive portal validation if WLAN authentication fails (applicable to EAP or MAC authentication only) |

#### Examples

```
nx9500-6C8809(config-wlan-test)#captive-portal-enforcement fall-back
nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type eap
 accounting syslog host 172.16.10.4 port 2
captive-portal-enforcement fall-back
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 broadcast-dhcp validate-offer
nx9500-6C8809(config-wlan-test)#
```

#### Related Commands

|                 |                                     |
|-----------------|-------------------------------------|
| <code>no</code> | Disables captive portal enforcement |
|-----------------|-------------------------------------|

### client-access

Enables WLAN client access (for normal data operations)

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

`client-access`

#### Parameters

None

#### Examples

```
nx9500-6C8809(config-wlan-1)#client-access
nx9500-6C8809(config-wlan-1)#
```

### client-client-communication

Allows frame switching from one client to another on a WLAN

This option is enabled by default. It allows clients to exchange packets with other clients. It does not necessarily prevent clients on other WLANs from sending packets to this WLAN, but as long as this setting is also disabled on that WLAN, clients are not permitted to interoperate.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
client-client-communication
```

#### Parameters

None

#### Examples

```
nx9500-6C8809(config-wlan-1)#client-client-communication
nx9500-6C8809(config-wlan-1)#
```

#### Related Commands

|                 |                                                               |
|-----------------|---------------------------------------------------------------|
| <code>no</code> | Disables frame switching from one client to another on a WLAN |
|-----------------|---------------------------------------------------------------|

### client-load-balancing

Enforces client load balancing on a WLAN's access point radios. When enforced, probe and association requests are not responded to, forcing a client to associate with another access point radio.

This feature is disabled by default.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
client-load-balancing {allow-single-band-clients|band-discovery-intvl|
capability-ageout-time|max-probe-req|probe-req-intvl}
client-load-balancing {allow-single-band-clients [2.4ghz|5ghz]|band-discovery-intvl
<0-10000>/capability-ageout-time <0-10000>}
client-load-balancing {max-probe-req|probe-req-intvl} [2.4ghz|5ghz] <0-10000>
```

#### Parameters

```
client-load-balancing {allow-single-band-clients [2.4ghz|5ghz]|band-discovery-intvl
<0-10000>/capability-ageout-time <0-10000>}
```

|                                            |                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| client-load-balancing                      | Configures client load balancing on a WLAN                                                                                                                                                                                                                                                                          |
| allow-single-band-clients<br>[2.4GHz 5GHz] | Optional. Allows single band clients to associate even during load balancing <ul style="list-style-type: none"><li>• 2.4GHz – Enables load balancing across 2.4 GHz channels</li><li>• 5GHz – Enables load balancing across 5.0 GHz channels</li></ul> This option is enabled by default for 2.4 and 5.0 GHz bands. |

|                                     |                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| band-discovery-intvl<br><0-10000>   | Optional. Configures time interval to discover a client's band capability before connection <ul style="list-style-type: none"> <li>&lt;0-10000&gt; - Specify a value from 0 - 10000 seconds. The default is 10 seconds.</li> </ul>                                                                                                                                      |
| capability-ageout-time<br><0-10000> | Optional. Configures a client's capability ageout interval. This is the time for which a client's capabilities are retained in the device's internal table. Once this time is exceeded the client's capabilities are aged out. <ul style="list-style-type: none"> <li>&lt;0-10000&gt; - Specify a value from 0 - 10000 seconds. The default is 3600 seconds.</li> </ul> |

`client-load-balancing {max-probe-req/probe-req-intvl} [2.4Ghz|5Ghz] <0-10000>`

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| client-load-balancing                  | Configures WLAN client load balancing                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| max-probe-req [2.4GHz 5GHz] <0-10000>  | Optional. Configures the maximum client probe requests allowed for 2.4 GHz and 5.0 GHz bands <ul style="list-style-type: none"> <li>2.4GHz - Configures maximum client probe requests on 2.4 GHz radios</li> <li>5GHz - Configures maximum client probe requests on 5.0 GHz radios <ul style="list-style-type: none"> <li>&lt;0-10000&gt; - Specify a client probe request threshold from 0 - 10000. The default for both 2.4 and 5.0 GHz radios is 60.</li> </ul> </li> </ul> |
| probe-req-intvl 2.4GHz 5GHz] <0-10000> | Optional. Configures client probe request interval limits for device association <ul style="list-style-type: none"> <li>2.4GHz - Configures the client probe request interval on 2.4 GHz radios</li> <li>5GHz - Configures the client probe request interval on 5.0 GHz radios <ul style="list-style-type: none"> <li>&lt;0-10000&gt; - Specify a value from 0 - 10000. The default for both 2.4 and 5.0 GHz radios is 10 seconds.</li> </ul> </li> </ul>                      |

### Examples

```

nx9500-6C8809(config-wlan-test)#client-load-balancing band-discovery-intvl 2
nx9500-6C8809(config-wlan-test)#client-load-balancing probe-req-intvl 5ghz 5
nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type eap
 accounting syslog host 172.16.10.4 port 2
 client-load-balancing probe-req-intvl 5ghz 5
client-load-balancing band-discovery-intvl 2
 captive-portal-enforcement fall-back
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 broadcast-dhcp validate-offer
nx9500-6C8809(config-wlan-test)#

```

### Related Commands

|                 |                                                                |
|-----------------|----------------------------------------------------------------|
| <code>no</code> | Disables client load balancing on a WLAN's access point radios |
|-----------------|----------------------------------------------------------------|

### controller-assisted-mobility

Enables controller or service platform assisted mobility to determine a wireless client's VLAN assignment. When enabled, a controller or service platform's mobility database is used to assist in roaming between RF Domains. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

`controller-assisted-mobility`

#### Parameters

None

#### Examples

```
rfs4000-229D58(config-wlan-test)#controller-assisted-mobility
rfs4000-229D58(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 controller-assisted-mobility
rfs4000-229D58(config-wlan-test)#
```

#### Related Commands

|                 |                                                                                                            |
|-----------------|------------------------------------------------------------------------------------------------------------|
| <code>no</code> | Disables controller or service platform assisted mobility to determine a wireless client's VLAN assignment |
|-----------------|------------------------------------------------------------------------------------------------------------|

## data-rates

Specifies the 802.11 rates supported on a WLAN

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
data-rates [2.4GHz|5GHz]
data-rates 2.4GHz [b-only|bg|bgn|custom|default|g-only|gn]
data-rates 2.4GHz custom [1|11|12|18|2|24|36|48|5.5|54|6|9|basic-1|basic-11|
basic-12|basic-18|basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|basic-6|basic-9|
basic-mcs-1s|mcs-1s|mcs-2s|mcs-3s]
data-rates 5GHz [a-only|an|custom|default]
data-rates 5GHz custom [12|18|24|36|48|54|6|9|basic-1|basic-11|basic-12|
basic-18|basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|basic-6|basic-9|
basic-mcs-1s|mcs-1s|mcs2s|mcs3s]
```

#### Parameters

`data-rates 2.4GHz [b-only|bg|bgn|default|g-only|gn]`

|                         |                                                                     |
|-------------------------|---------------------------------------------------------------------|
| <code>data-rates</code> | Specifies the 802.11 rates supported when mapped to a 2.4 GHz radio |
| <code>b-only</code>     | Uses rates that support only 11b clients                            |
| <code>bg</code>         | Uses rates that support both 11b and 11g clients                    |
| <code>bgn</code>        | Uses rates that support 11b, 11g and 11n clients                    |
| <code>default</code>    | Uses the default rates configured for a 2.4 GHz radio               |

|        |                                               |
|--------|-----------------------------------------------|
| g-only | Uses rates that support operation in 11g only |
| gn     | Uses rates that support 11g and 11n clients   |

`data-rates 5GHz [a-only|an|default]`

|            |                                                                     |
|------------|---------------------------------------------------------------------|
| data-rates | Specifies the 802.11 rates supported when mapped to a 5.0 GHz radio |
| a-only     | Uses rates that support operation in 11a only                       |
| an         | Uses rates that support 11a and 11n clients                         |
| default    | Uses default rates configured for a 5.0 GHz                         |

`data-rates [2.4GHz|5GHz] custom [1|11|12|18|2|24|36|48|5.5|54|6|9|basic-1|basic-11|basic-12|basic-18|basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|basic-6|basic-9|basic-mcs0-7|mcs0-15|mcs0-7|mcs8-15]`

|                          |                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| data-rates [2.4GHz 5GHz] | Specifies the 802.11 rates supported when mapped to a 2.4 GHz or 5.0 GHz radio                                                                                                                                                                                                                                                                                   |
| custom                   | Configures a data rates list by specifying each rate individually. Use 'basic-' prefix before a rate to indicate it is used as a basic rate (For example, 'data-rates custom basic-1 basic-2 5.5 11').<br>The data-rates for 2.4 GHz and 5.0 GHz channels are the same with a few exceptions. The 2.4 GHz channel has a few extra data rates: 1, 11, 2, and 5.5. |



|                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1,11,2,5.5                                                                                                                                                         | The following data rates are specific to the 2.4 GHz channel: <ul style="list-style-type: none"> <li>• 1 – 1-Mbps</li> <li>• 11 – 11-Mbps</li> <li>• 2 – 2-Mbps</li> <li>• 5.5 – 5.5-Mbps</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 12,18,24,36,48,54,6,9, basic-1,basic-11, basic-12,basic-18, basic-2, basic-36,basic-48, basic-5.5, basic-54,basic-6, basic-9, basic-mcs0-7,mcs0-15, mcs0-7,mcs8-15 | The following data rates are common to both the 2.4 GHz and 5.0 GHz channels: <ul style="list-style-type: none"> <li>• 12 – 12 Mbps</li> <li>• 18 – 18-Mbps</li> <li>• 24 – 24 Mbps</li> <li>• 36 – 36-Mbps</li> <li>• 48 – 48-Mbps</li> <li>• 54 – 54-Mbps</li> <li>• 6 – 6-Mbps</li> <li>• 9 – 9-Mbps</li> <li>• basic-1 – basic 1-Mbps</li> <li>• basic-11 – basic 11-Mbps</li> <li>• basic-12 – basic 12-Mbps</li> <li>• basic-18 – basic 18-Mbps</li> <li>• basic-2 – basic 2-Mbps</li> <li>• basic-36 – basic 36-Mbps</li> <li>• basic-48 – basic 48-Mbps</li> <li>• basic-5.5 – basic 5.5-Mbps</li> <li>• basic-54 – basic 54-Mbps</li> <li>• basic-6 – basic 6-Mbps</li> <li>• basic-9 – basic 9-Mbps</li> <li>• basic-mcs-1s – Modulation and coding scheme data rates for 1 Spatial Stream</li> <li>• mcs-1s – Applicable to 1-spatial stream data rates</li> <li>• mcs-2s – Applicable to 2-spatial stream data rates</li> <li>• mcs-3s – Applicable to 3-spatial stream data rates</li> </ul> |

### Examples

```

nx9500-6C8809(config-wlan-test)#data-rates 2.4GHz gn
nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type eap
 accounting syslog host 172.16.10.4 port 2
 data-rates 2.4GHz gn
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 captive-portal-enforcement fall-back
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 broadcast-dhcp validate-offer
nx9500-6C8809(config-wlan-test)#

```

### Related Commands

|           |                                                                                    |
|-----------|------------------------------------------------------------------------------------|
| <b>no</b> | Resets the 802.11 data rates supported on a WLAN for the 2.4 GHz or 5.0 GHz radios |
|-----------|------------------------------------------------------------------------------------|

## description

Configures a description for this WLAN

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
description <LINE>
```

### Parameters

```
description <LINE>
```

<LINE> Specify a description for this WLAN  
The WLAN's description should help differentiate it from others with similar configurations. The description should not exceed 64 characters.

### Examples

```
nx9500-6C8809(config-wlan-test)#description TestWLAN
nx9500-6C8809(config-wlan-test)#show context
wlan test
 description TestWLAN
 ssid test
 bridging-mode local
 encryption-type none
 uthentication-type eap
 accounting syslog host 172.16.10.4 port 2
 data-rates 2.4GHz gn
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 captive-portal-enforcement fall-back
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 broadcast-dhcp validate-offer
nx9500-6C8809(config-wlan-test)#
```

### Related Commands

**no** Removes a WLAN's configured description

## downstream-group-addressed-forwarding

Enables forwarding of downstream broadcast/multicast (BC/MC) packets to a group on this WLAN. This feature is enabled by default.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
downstream-group-addressed-forwarding
```

### Parameters

None

## Examples

```
rfs4000-229D58(config-wlan-test)#downstream-group-addressed-forwarding
```

## Related Commands

|                 |                                                                        |
|-----------------|------------------------------------------------------------------------|
| <code>no</code> | Disables forwarding of downstream BCMC packets to a group on this WLAN |
|-----------------|------------------------------------------------------------------------|

## dpi

Enables DPI on this WLAN. When enabled, all traffic is subjected to DPI for detection of applications, application categories, custom applications, and metadata extraction.

DPI is an advanced packet analysis technique, which analyzes packet and packet content headers to determine the nature of network traffic. When enabled, DPI inspects packets of all flows to identify applications (such as, Netflix, Twitter, Facebook, etc.) and extract metadata (such as, host name, server name, TCP-RTT, etc.) for further use by the WiNG firewall.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
dpi metadata [http|ssl|tcp-rtt|voice-video]
```

## Parameters

```
dpi metadata [http|ssl|tcp-rtt|voice-video]
```

|                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>dpi metadata [http ssl tcp-rtt voice-video]</code> | <p>Enables extraction of the following metadata flows:</p> <ul style="list-style-type: none"><li>• <code>http</code> – Extracts HTTP flows. When enabled, administrators can track HTTP Websites accessed by both internal and guest clients and visualize HTTP data usage, hits, active time and total clients on the NSight application's dashboard. This setting is disabled by default.</li><li>• <code>ssl</code> – Extracts SSL flows. When enabled, administrators can track SSL Websites accessed by both internal and guest clients and visualize SSL data usage, hits, active time and total clients on the NSight application's dashboard. This setting is disabled by default</li><li>• <code>tcp-rtt</code> – Extracts RTT (Round Trip Time) information from TCP (Transmission Control Protocol) flows. However, this TCP-RTT metadata is viewable only on the NSight dashboard. Therefore, ensure the NSight server is up and NSight analytics data collection is enabled.</li><li>• <code>voice-video</code> – Extracts voice and video flows. When enabled, voice and video calls can be tracked by extracting parameters, such as packets transferred and lost, jitter, and application name. Most Enterprise VoIP applications like facetime, skype for business and VoIP terminals can be monitored for call quality and visualized on the NSight dashboard in manner similar to HTTP and SSL. Call quality and metrics can only be determined from calls established unencrypted. This setting is disabled by default.</li></ul> |
|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-wlan-test)#dpi metadata http
nx9500-6C8809(config-wlan-test)#dpi metadata ssl
nx9500-6C8809(config-wlan-test)#dpi metadata voice-video
nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 dpi metadata voice-video
 dpi metadata http
 dpi metadata ssl
nx9500-6C8809(config-wlan-test)#
```

## Related Commands

|                 |                                                   |
|-----------------|---------------------------------------------------|
| <code>no</code> | Disables extraction of metadata flows on the WLAN |
|-----------------|---------------------------------------------------|

## dynamic-vlan-assignment

Enables dynamic VLAN assignment on this WLAN, and adds or removes VLANs for the selected WLAN. Configure this feature to allow an override to the WLAN configuration. If, as part of the authentication process, the RADIUS server returns a client's VLAN-ID in a RADIUS Access-Accept packet, and this feature is enabled, all client traffic is forward on that VLAN. If disabled, the RADIUS server returns VLAN-ID is ignored and the WLAN's VLAN configuration is used. For more information, see [vlan](#). This option is disabled by default.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
dynamic-vlan-assignment allowed-vlan <VLAN-ID>
```

## Parameters

```
dynamic-vlan-assignment allowed-vlan <VLAN-ID>
```

|                                      |                                                                                                                                                                                                    |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dynamic-vlan-assignment allowed-vlan | Enables dynamic VLAN assignment and configures a list of VLAN IDs or VLAN alias allowed access to the WLAN                                                                                         |
| <VLAN-ID>                            | Specify the list of VLAN IDs or the VLAN alias names. For example, 10-20, 25, 30-35, \$guest. For example, 10-20, 25, 30-35, \$guest. For information on VLAN aliases, see <a href="#">alias</a> . |

## Examples

```
rfs4000-229D58(config-wlan-test)#dynamic-vlan-assignment allowed-vlans 10-20
rfs4000-229D58(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 dynamic-vlan-assignment allowed-vlans 10-20
rfs4000-229D58(config-wlan-test)#
```

## Related Commands

|           |                                               |
|-----------|-----------------------------------------------|
| <b>no</b> | Disables dynamic VLAN assignment on this WLAN |
|-----------|-----------------------------------------------|

### eap-types

Configures client access based on the EAP type used

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
eap-types [allow|deny] [aka|all|fast|peap|sim|tls|ttls] {(aka|all|fast|peap|sim|tls|ttls)}
```

### Parameters

```
eap-types [allow|deny] [aka|all|fast|peap|sim|tls|ttls] {(aka|all|fast|peap|sim|tls|ttls)}
```

|                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| eap-types                        | Configures a list of allowed or denied EAP types                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| [allow deny]                     | <ul style="list-style-type: none"><li>• allow – Configures a list of EAP types allowed for WLAN client authentication</li><li>• deny – Configures a list of EAP types not allowed for WLAN client authentication</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| [aka all fast peap sim tls ttls] | <p>The following EAP types are common to the 'allow' and 'deny' keywords:</p> <ul style="list-style-type: none"><li>• aka – Configures EAP AKA (Authentication and Key Agreement ) and EAP-AKA' (AKA Prime). EAP-AKA is one of the methods in the EAP authentication framework. It uses UMTS (Universal Mobile Telecommunications System) and USIM (Universal Subscriber Identity Module) for client authentication and key distribution.</li><li>• all – Allows or denies usage of all EAP types on the WLAN</li><li>• fast – Configures EAP FAST (Flexible Authentication via Secure Tunneling). EAP-FAST establishes a TLS (Transport Layer Security ) tunnel, to verify client credentials, using PAC (Protected Access Credentials).</li><li>• peap – Configures PEAP (Protected Extensible Authentication Protocol). PEAP or Protected EAP uses encrypted and authenticated TLS tunnel to encapsulate EAP.</li><li>• sim – Configures EAP SIM (Subscriber Identity Module). EAP-SIM uses GSMC (Global System for Mobile Communications) SIM for client authentication and key distribution.</li><li>• tls – Configures EAP TLS. EAP-TLS is an EAP authentication method that uses PKI to communicate with a RADIUS server or any other authentication server.</li><li>• ttls – Configures TTLS (Tunneled Transport Layer Security). EAP-TTLS is an extension of TLS. Unlike TLS, TTLS does not require every client to generate and install a CA-signed certificate.</li><li>• These options are recursive, and more than one EAP type can be selected. The selected options are added to the allowed or denied EAP types list.</li></ul> |

### Examples

```
nx9500-6C8809(config-wlan-test)#eap-types allow fast sim tls
nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 eap-types allow fast sim tls
nx9500-6C8809(config-wlan-test)#
```

## Related Commands

|                 |                                                  |
|-----------------|--------------------------------------------------|
| <code>no</code> | Reverts to default setting - eap-types allow all |
|-----------------|--------------------------------------------------|

## encryption-type

Sets a WLAN's encryption type

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
encryption-type [ccmp|keyguard|none|tkip-ccmp|wep128|wep128-keyguard|wep64]
```

## Parameters

```
encryption-type [ccmp|keyguard|none|tkip-ccmp|wep128|wep128-keyguard|wep64]
```

|                 |                                                                                                                                                                     |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| encryption-type | Configures the WLAN's data encryption parameters                                                                                                                    |
| ccmp            | Configures AES-CCM/CCMP (Advanced Encryption Standard Counter Mode CBC-MAC Protocol)                                                                                |
| keyguard        | Configures Keyguard MCM (Mobile Computing Mode)                                                                                                                     |
| tkip-ccmp       | Configures the TKIP and AES-CCM/CCMP encryption modes                                                                                                               |
| wep128          | Configures WEP with 128 bit keys                                                                                                                                    |
| wep128-keyguard | Configures WEP128 as well as Keyguard-MCM encryption modes                                                                                                          |
| wep64           | Configures WEP with 64 bit keys. A WEP64 configuration is insecure when two WLANs are mapped to the same VLAN, and one uses no encryption while the other uses WEP. |

## Examples

```
nx9500-6C8809(config-wlan-test)#encryption-type tkip-ccmp
nx9500-6C8809(config-wlan-test)#show context
wlan test
 description TestWLAN
 ssid test
 bridging-mode local
encryption-type tkip-ccmp
 authentication-type eap
 accounting syslog host 172.16.10.4 port 2
 data-rates 2.4GHz gn
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 captive-portal-enforcement fall-back
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 broadcast-dhcp validate-offer
nx9500-6C8809(config-wlan-test)#
```

## Related Commands

|                 |                                                     |
|-----------------|-----------------------------------------------------|
| <code>no</code> | Resets the WLAN's encryption type to default (none) |
|-----------------|-----------------------------------------------------|

## enforce-dhcp

Enables dropping of packets from clients with a static IP address. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

`enforce-dhcp`

Parameters

None

Examples

```
nx9500-6C8809(config-wlan-test)#enforce-dhcp
nx9500-6C8809(config-wlan-test)#show context
wlan test
 description TestWLAN
 ssid test
 bridging-mode local
 encryption-type tkip-ccmp
 authentication-type eap
 accounting syslog host 172.16.10.4 port 2
 data-rates 2.4GHz gn
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 captive-portal-enforcement fall-back
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 enforce-dhcp
 broadcast-dhcp validate-offer
nx9500-6C8809(config-wlan-test)#
```

Related Commands

|                 |                                                                    |
|-----------------|--------------------------------------------------------------------|
| <code>no</code> | Disables dropping of packets from clients with a static IP address |
|-----------------|--------------------------------------------------------------------|

fast-bss-transition

Enables or disables support for 802.11r FT (Fast-BSS Transition) on the selected WLAN. This feature is disabled by default.

802.11r is an attempt to undo the burden that security and QoS added to the handoff process, and restore it back to an original four message exchange process. The central application for the 802.11r standard is VOIP using mobile phones within wireless Internet networks. 802.11r FT redefines the security key negotiation protocol, allowing parallel processing of negotiation and requests for wireless resources.

Enabling FT standards provides wireless clients fast, secure and seamless transfer from one base station to another, ensuring continuous connectivity.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
fast-bss-transition {over-ds}
```

## Parameters

```
fast-bss-transition {over-ds}
```

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| fast-bss-transition over-ds | Enables 802.11r FT support on this WLAN <ul style="list-style-type: none"><li>over-ds - Optional. Enables 802.11r client roaming over the DS (Distribution System). When enabled, all client communication with the target AP is via the current AP. This communication, carried in FT action frames, is first sent by the client to the current AP, then forwarded to the target AP through the controller.</li></ul> |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-wlan-test)#fast-bss-transition
<exsw1>(config-wlan-test)#show context
wlan test
 ssid test
 vlan 1
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 fast-bss-transition
nx9500-6C8809(config-wlan-test)#
```

## Related Commands

|    |                                                                 |
|----|-----------------------------------------------------------------|
| no | Disables support for 802.11r Fast-BSS Transition (FT) on a WLAN |
|----|-----------------------------------------------------------------|

## http-analyze

Enables HTTP URL analysis on the WLAN

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
http-analyze [filter|syslog]
http-analyze filter [images|post|query-string]
http-analyze syslog host <IP/HOSTNAME> {port <1-65535>}
{proxy-mode [none|through-controller|through-rf-domain-manager]}
```

## Parameters

```
http-analyze filter [images|post|query-string]
```

|              |                                                                                                                             |
|--------------|-----------------------------------------------------------------------------------------------------------------------------|
| filter       | Filters URLs, based on the parameters set, before forwarding them                                                           |
| images       | Filters out URLs referring to images (does not forward URL requesting images)                                               |
| post         | Filters out URLs requesting POST (does not forward POST requests). This option is disabled by default.                      |
| query-string | Removes query strings from URLs before forwarding them (forwards requests and no data). This option is disabled by default. |

```
http-analyze syslog host <IP/HOSTNAME> {port <1-65535>}
{proxy-mode [none|through-controller|through-rf-domain-manager]}
```



|                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| syslog host <IP/<br>HOSTNAME>                                           | Forwards client and URL information to a syslog server <ul style="list-style-type: none"> <li>host &lt;IP/HOSTNAME&gt; – Specify the syslog server's IP address or hostname</li> </ul>                                                                                                                                                                                                          |
| port <1-65535>                                                          | Optional. Specifies the UDP port to connect to the syslog server from 1 - 65535                                                                                                                                                                                                                                                                                                                 |
| proxy-mode [none through-<br>controller  through-rf-<br>domain-manager] | Optional. Specifies if the request is to be proxied through another device <ul style="list-style-type: none"> <li>none – Requests are sent directly to syslog server from device</li> <li>through-controller – Proxies requests through the wireless controller configuring the device</li> <li>through-rf-domain-manager – Proxies the requests through the local RF Domain manager</li> </ul> |

### Examples

```
rfs4000-229D58(config-wlan-test)#http-analyze syslog host 192.168.13.10 port 21
proxy-mode through-controller
rfs4000-229D58(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 http-analyze syslog host 192.168.13.10 port 21 proxy-mode through-controller
rfs4000-229D58(config-wlan-test)#
```

### Related Commands

|           |                                        |
|-----------|----------------------------------------|
| <b>no</b> | Disables HTTP URL analysis on the WLAN |
|-----------|----------------------------------------|

## ip (wlan-config-mode)

Configures IP settings

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
ip [arp|dhcp]
ip arp [header-mismatch-validation|trust]
ip dhcp trust
```

### Parameters

```
ip arp [header-mismatch-validation|trust]
```

|                                |                                                                                                             |
|--------------------------------|-------------------------------------------------------------------------------------------------------------|
| ip arp                         | Configures the IP settings for ARP packets                                                                  |
| header-mismatch-<br>validation | Verifies mismatch of source MAC address in the ARP and Ethernet headers. This option is enabled by default. |
| trust                          | Sets ARP responses as trusted for a WLAN/range. This option is disabled by default.                         |

```
ip dhcp trust
```

|         |                                                                                      |
|---------|--------------------------------------------------------------------------------------|
| ip dhcp | Configures the IP settings for DHCP packets                                          |
| trust   | Sets DHCP responses as trusted for a WLAN/range. This option is disabled by default. |

Examples

```

nx9500-6C8809(config-wlan-test)#ip dhcp trust
<exsw1>(config-wlan-test)#show context
wlan test
 description TestWLAN
 ssid test
 bridging-mode local
 encryption-type tkip-ccmp
 authentication-type eap
 accounting syslog host 172.16.10.4 port 2
 data-rates 2.4GHz gn
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 captive-portal-enforcement fall-back
 ip dhcp trust
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 enforce-dhcp
 broadcast-dhcp validate-offer
 http-analyze controller
nx9500-6C8809(config-wlan-test)#

```

Related Commands

|    |                                                                                                                                            |
|----|--------------------------------------------------------------------------------------------------------------------------------------------|
| no | Resets IP ARP or DHCP trust parameters to default. ARP trust is disabled, ARP mismatch verification is enabled, or DHCP trust is disabled. |
|----|--------------------------------------------------------------------------------------------------------------------------------------------|

ipv6

Sets the DHCPv6 and ICMPv6 ND (neighbor discovery) components for this WLAN

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```

ipv6 [dhcpv6|nd]
ipv6 dhcpv6 trust
ipv6 nd [header-mismatch-validation|ranguard|trust]

```

Parameters

```

ipv6 dhcpv6 trust

```

|                   |                                                                                                                                                                                       |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ipv6 dhcpv6 trust | Enables DHCPv6 trust state for DHCPv6 responses on this WLAN. When enabled, all DHCPv6 responses received on this WLAN are trusted and forwarded. This option is disabled by default. |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```

ipv6 nd [header-mismatch-validation|ranguard|trust]

```

|                            |                                                                                                                                                |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| ipv6 nd                    | Sets the IPv6 ND settings for this WLAN                                                                                                        |
| header-mismatch-validation | Checks for mismatch of source MAC address in the ICMPv6 ND message and Ethernet header (link layer option). This option is enabled by default. |



|         |                                                                                                                                                                              |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| raguard | Allows redirection of router advertisements (RAs) and ICMPv6 packets originating on this WLAN. This option is disabled by default.                                           |
| trust   | Enables trust state for ND requests received on this WLAN. When enabled, all ND requests on an IPv6 firewall, on this WLAN, are trusted. This option is disabled by default. |

### Examples

```

nx9500-6C8809(config-wlan-test)#ipv6 dhcpv6 trust
nx9500-6C8809(config-wlan-test)#ipv6 nd trust
nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid test
 vlan 1
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 ipv6 dhcpv6 trust
 ipv6 nd trust
nx9500-6C8809(config-wlan-test)#

```

### Related Commands

|    |                                                                                                                                                                                                        |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| no | Resets IPv6 ND or DHCPv6 trust parameters to default. ND request trust is disabled, ND header mismatch verification is enabled, ND RA and ICMPv6 redirection is disabled, or DHCPv6 trust is disabled. |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## kerberos

Configures Kerberos authentication parameters on a WLAN

Kerberos (designed and developed by MIT) provides strong authentication for client/server applications using secret-key cryptography. Using Kerberos, a client must prove its identity to a server (and vice versa) across an insecure network connection.

Once a client and server use Kerberos to validate their identity, they encrypt all communications to assure privacy and data integrity. Kerberos can only be used on the access point with 802.11b clients. Kerberos uses NTP for synchronizing the clocks of its KDC server(s).

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```

kerberos [password|realm|server]
kerberos password [0 <LINE>|2 <LINE>|<LINE>]
kerberos realm <REALM>
kerberos server [primary|secondary|timeout]
kerberos server [primary|secondary] host <IP/HOSTNAME> {port <1-65535>}
kerberos server timeout <1-60>

```

### Parameters

```

kerberos password [0 <LINE>|2 <LINE>|<LINE>]

```

|          |                                                                                                                                                                                                                                                                                                                                        |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| kerberos | Configures a WLAN's Kerberos authentication parameters<br>The parameters are: password, realm, and server.                                                                                                                                                                                                                             |
| password | Configures a Kerberos KDC server password. The password should not exceed 127 characters. The password options are: <ul style="list-style-type: none"> <li>• 0 &lt;LINE&gt; – Configures a clear text password</li> <li>• 2 &lt;LINE&gt; – Configures an encrypted password</li> <li>• &lt;LINE&gt; – Specify the password.</li> </ul> |

kerberos realm <REALM>

|               |                                                                                                            |
|---------------|------------------------------------------------------------------------------------------------------------|
| kerberos      | Configures a WLAN's Kerberos authentication parameters<br>The parameters are: password, realm, and server. |
| realm <REALM> | Configures a Kerberos KDC server realm. The REALM should not exceed 127 characters.                        |

kerberos server [primary|secondary] host <IP/HOSTNAME> {port <1-65535>}

|                            |                                                                                                                                                                                                                                             |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| kerberos                   | Configures a WLAN's Kerberos authentication parameters<br>The parameters are: password, realm, and server.                                                                                                                                  |
| server [primary secondary] | Configures the primary and secondary KDC server parameters <ul style="list-style-type: none"> <li>• primary – Configures the primary KDC server parameters</li> <li>• secondary – Configures the secondary KDC server parameters</li> </ul> |
| host <IP/HOSTNAME>         | Sets the primary or secondary KDC server address <ul style="list-style-type: none"> <li>• &lt;IP/HOSTNAME&gt; – Specify the IP address or name of the KDC server.</li> </ul>                                                                |
| port <1-65535>             | Optional. Configures the UDP port used to connect to the KDC server <ul style="list-style-type: none"> <li>• &lt;1-65535&gt; – Specify the port from 1 - 65535. The default is 88.</li> </ul>                                               |

kerberos server timeout <1-60>

|                |                                                                                                                                                                                                                                                    |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| kerberos       | Configures a WLAN's Kerberos authentication parameters<br>The parameters are: password, realm, and server.                                                                                                                                         |
| timeout <1-60> | Modifies the Kerberos KDC server's timeout parameters <ul style="list-style-type: none"> <li>• &lt;1-60&gt; – Specifies the wait time for a response from the Kerberos KDC server before retrying. Specify a value from 1 - 60 seconds.</li> </ul> |

### Examples

```

nx9500-6C8809(config-wlan-test)#kerberos server timeout 12
<exsw1>(config-wlan-test)#kerberos server primary host 172.16.10.2 port 88
nx9500-6C8809(config-wlan-test)#show context
wlan test
description TestWLAN
ssid test
bridging-mode local
encryption-type tkip-ccmp
authentication-type eap
kerberos server timeout 12
kerberos server primary host 172.16.10.2
accounting syslog host 172.16.10.4 port 2
data-rates 2.4GHz gn
client-load-balancing probe-req-intvl 5ghz 5
client-load-balancing band-discovery-intvl 2
captive-portal-enforcement fall-back

```

```

ip dhcp trust
acl exceed-rate wireless-client-denied-traffic 20 disassociate
enforce-dhcp
broadcast-dhcp validate-offer
http-analyze controller
nx9500-6C8809(config-wlan-test)#

```

#### Related Commands

|           |                                                              |
|-----------|--------------------------------------------------------------|
| <b>no</b> | Removes Kerberos authentication related parameters on a WLAN |
|-----------|--------------------------------------------------------------|

### mac-authentication

Enables MAC authentication. When enabled, the system uses cached credentials (RADIUS server lookups are skipped) to authenticate clients.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
mac-authentication [cached-credentials|enforce-always]
```

#### Parameters

```
mac-authentication [cached-credentials|enforce-always]
```

|                    |                                                                                                                                                                                                                                                                        |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mac-authentication | Enables MAC authentication on this WLAN and configures related parameters                                                                                                                                                                                              |
| cached-credentials | Uses cached credentials to skip RADIUS lookups. This option is disabled by default.                                                                                                                                                                                    |
| enforce-always     | Enforces MAC authentication on this WLAN. When enabled, MAC authentication is enforced, each time a client logs in, even when the authentication type specified (using the authentication-type command) is not MAC authentication. This option is disabled by default. |

#### Examples

```

rfs4000-229D58(config-wlan-test)#mac-authentication cached-credentials
rfs4000-229D58(config-wlan-test)#

```

#### Related Commands

|           |                                                                                                                                                                        |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>no</b> | Disables MAC authentication related parameters: Disables use of cached credentials to skip RADIUS lookups, or disables enforcement of MAC authentication on this WLAN. |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### nsight

Enables retention of client-history

A typical NSight-server enabled, guest access environment may be visited by thousands of unique clients on a daily basis. Some of these guest clients are not regular visitors, accessing the network infrequently. However, by default, historical data of all guest clients, irrespective of their network access frequency, is retained by the NSight server for up to 180 days. This results in the database containing thousands if not millions of unique MAC addresses of infrequent guest clients. To address this potential problem it is recommended to disable client-history retention on a guest WLAN, and use the nsight-

policy context to configure a separate timer (8 hours by default) specifying the guest client data lifespan in the database.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
nsight client-history
```

#### Parameters

```
nsight client-history
```

|                       |                                                                                         |
|-----------------------|-----------------------------------------------------------------------------------------|
| nsight client-history | Enables retention of client-history in the database. This option is enabled by default. |
|-----------------------|-----------------------------------------------------------------------------------------|

#### Examples

On a WLAN, the client-history option is enabled by default. When enabled, all client history (including guest-clients) is retained in the NSight server database for 180 days.

To disable this option, execute the **no > nsight > client-history** command. When disabled, guest client history is retained only for 8 hours, which is the default setting defined by the NSight policy applied on the access point (through which the guest client accesses the WLAN) or the access point's RF Domain. However, the default historical data retention duration for regular clients and devices (access point and controllers) remains unchanged (180 days) as per the NSight policy settings.

```
nx9500-6C8809(config-wlan-test3)#no nsight client-history
nx9500-6C8809(config-wlan-test3)#show context
wlan test3
 ssid test3
 bridging-mode local
 encryption-type none
 authentication-type none
 no nsight client-history
nx9500-6C8809(config-wlan-test3)#
```

Use the NSight policy context to define separate client-history retention time for regular clients, devices, and guest clients. For more information, see

#### Related Commands

|    |                                                          |
|----|----------------------------------------------------------|
| no | Disables client-history retention in the NSight database |
|----|----------------------------------------------------------|

#### opendns

Configures the pre-fetched OpenDNS device\_id. Once configured, all DNS queries originating from wireless clients associating with the WLAN are appended with an additional 31 bytes of data (representing the device ID) at the end of the DNS packet. The device ID is a sixteen (16) character hex string representing a 64 bit unsigned integer and is fetched from the OpenDNS site.

This command is part of a series of configurations that are required to integrate WiNG access points, wireless controllers, and service platforms with OpenDNS. When all the parameters have been configured, DNS queries from wireless clients, associating with the WLAN, are redirected to OpenDNS

(208.67.220.220 OR 208.67.222.222). These OpenDNS resolvers act as proxy DNS servers that provide additional functionalities, such as Web filtering, reporting, and performance enhancement. For more information on the entire configuration, see [opendns](#) (privi exec mode).

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
opendns device-id <DEVICE-ID>
```

#### Parameters

```
opendns device-id <DEVICE-ID>
```

|                                                |                                                                                                                                                               |
|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>opendns device-id &lt;DEVICE-ID&gt;</pre> | Configures the device ID to embed in DNS queries sent to OpenDNS <ul style="list-style-type: none"><li>• &lt;DEVICE-ID&gt; - Specify the device ID.</li></ul> |
|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

The following command fetches the device\_id from the OpenDNS site.

```
ap7161-E6D512#opendns ApiToken 9110B39543DEB2ECA1F473AE03E8899C00019073
device_id = 0014AADF8EDC6C59
ap7161-E6D512#
```

Use this device\_id in the WLAN configuration context.

```
ap7161-E6D512(config)#wlan opendns
ap7161-E6D512(config-wlan-opendns)#opendns device-id 0014AADF8EDC6C59
ap7161-E6D512(config-wlan-opendns)#commit
ap7161-E6D512(config-wlan-opendns)#show context
wlan opendns
 ssid opendns
 vlan 1
 bridging-mode local
 encryption-type none
 authentication-type none
 opendns device-id 0014AADF8EDC6C59
ap7161-E6D512(config-wlan-opendns)#
```

#### Related Commands

|               |                                                                                                      |
|---------------|------------------------------------------------------------------------------------------------------|
| <pre>no</pre> | Removes the device ID configured to be embedded in the DNS queries originating from the WiNG devices |
|---------------|------------------------------------------------------------------------------------------------------|

#### protected-mgmt-frames

Configures the WLAN's frame protection mode and SA (security association) query parameters

802.11w provides protection for both unicast management frames and broadcast/multicast management frames. The 'robust management frames' are action, disassociation, and de-authentication frames. The standard provides one security protocol CCMP for protection of unicast robust management frames. PMF (Protected management frames) protocol only applies to robust management frames after establishment of RSNA PTK. Robust management frame protection is achieved by using CCMP for unicast management frames, broadcast/multicast integrity protocol for

broadcast/multicast management frames and SA query protocol for protection against (re)association attacks.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
protected-mgmt-frames [mandatory|optional|sa-query [attempts <1-10>|timeout <100-1000>]
```

#### Parameters

```
protected-mgmt-frames [mandatory|optional|sa-query [attempts <1-10>|timeout <100-1000>]
```

|                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| protected-mgmt-frames                             | Enables and configures WLAN's frame protection mode and SA query parameters. Use this command to specify whether management frames are continually or optionally protected. Frame protection mode is disabled by default.                                                                                                                                                                                                              |
| mandatory                                         | Enforces protected management frames (PMF) on this WLAN (management frames are continually optionally protected)                                                                                                                                                                                                                                                                                                                       |
| optional                                          | Provides PMF only for those clients that support PMF (management frames are optionally protected)                                                                                                                                                                                                                                                                                                                                      |
| sa-query [attempts <1-10> <br>timeout <100-1000>] | Configures the following SA parameters: <ul style="list-style-type: none"><li>• attempts &lt;1-10&gt; - Configures the number of SA query attempts from 1 - 10. The default is 5.</li><li>• timeout &lt;100-1000&gt; - Configures the interval, in milliseconds, used to timeout association requests that exceed the defined interval. Specify a value from 100 - 1000 milliseconds. The default value is 201 milliseconds.</li></ul> |

#### Examples

```
nx9500-6C8809(config-wlan-test)#protected-mgmt-frames mandatory
nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 protected-mgmt-frames mandatory
nx9500-6C8809(config-wlan-test)#
```

#### Related Commands

|    |                                                                                                                                                                                 |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| no | Disables enforcement of protected management frames on this WLAN. And reverts protected management frames sa-query timeout and attempts to 201 milliseconds and 5 respectively. |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### proxy-arp-mode

Enables proxy ARP mode for handling ARP requests

Proxy ARP is the technique used to answer ARP requests intended for another system. By faking its identity, the access point accepts responsibility for routing packets to the actual destination.

Supported in the following platforms:



- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
proxy-arp-mode [dynamic|strict]
```

#### Parameters

```
proxy-arp-mode [dynamic|strict]
```

|                |                                                                                                 |
|----------------|-------------------------------------------------------------------------------------------------|
| proxy-arp-mode | Enables proxy ARP mode for handling ARP requests. The options available are dynamic and strict. |
| dynamic        | Forwards ARP requests to the wireless side (for which a response could not be proxied)          |
| strict         | Does not forward ARP requests to the wireless side                                              |

#### Examples

```
nx9500-6C8809(config-wlan-test)#proxy-arp-mode strict
nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type none
 protected-mgmt-frames mandatory
 wing-extensions wmm-load-information
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 proxy-arp-mode strict
 broadcast-dhcp validate-offer
 http-analyze controller
nx9500-6C8809(config-wlan-test)#
```

#### Related Commands

|    |                                                 |
|----|-------------------------------------------------|
| no | Reverts the proxy ARP mode to default (dynamic) |
|----|-------------------------------------------------|

### proxy-nd-mode

Configures the proxy ND mode for this WLAN member clients as either strict or dynamic

ND proxy is used in IPv6 to provide reachability by allowing a client to act as proxy. Proxy certificate signing can be done either dynamically (requiring exchanges of identity and authorization information) or statically when the network topology is defined.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
proxy-nd-mode [dynamic|strict]
```

#### Parameters

```
proxy-nd-mode [dynamic|strict]
```

|                                |                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| proxy-nd-mode [dynamic strict] | Configures the proxy ND mode for this WLAN member clients. The options are: dynamic and strict <ul style="list-style-type: none"> <li>• dynamic - Forwards ND request to wireless for which a response could not be proxied. This is the default value.</li> <li>• strict - Does not forward ND requests to the wireless side</li> </ul> |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config-wlan-test)#proxy-nd-mode strict
nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 wpa-wpa2 server-only-authentication
 proxy-nd-mode strict
 .opendns device-id 44-55-66
nx9500-6C8809(config-wlan-test)#
```

### Related Commands

|    |                                                |
|----|------------------------------------------------|
| no | Reverts the proxy ND mode to default (dynamic) |
|----|------------------------------------------------|

## qos-map

Enables support for 802.11u QoS map element and frames

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

qos-map

### Parameters

None

### Examples

```
nx9500-6C8809(config-wlan-test)#qos-map
nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 qos-map
 wpa-wpa2 server-only-authentication
 proxy-nd-mode strict
 .opendns device-id 44-55-66
nx9500-6C8809(config-wlan-test)#
```

### Related Commands

|    |                                                         |
|----|---------------------------------------------------------|
| no | Disables support for 802.11u QoS map element and frames |
|----|---------------------------------------------------------|

## radio-resource-measurement

Enables support for 802.11k radio resource measurement capabilities (IEEE 802.11k) on this WLAN

802.11k improves how traffic is distributed. In a WLAN, devices normally connect to the access point with the strongest signal. Depending on the number and location of clients, this arrangement can lead to excessive demand on one access point and under utilization of others, resulting in degradation of overall network performance. With 802.11k, if the access point with the strongest signal is loaded to its capacity, a client connects to an under-utilized access point. Even if the signal is weaker, the overall throughput is greater since it's an efficient use of the network's resources. This feature is disabled by default.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
radio-resource-measurement {channel-report|neighbor-report {hybrid}}
```

#### Parameters

```
radio-resource-measurement {channel-report|neighbor-report {hybrid}}
```

|                            |                                                                                                                                                                                                              |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| radio-resource-measurement | Enables support for 802.11k radio resource measurement capabilities                                                                                                                                          |
| channel-report             | Optional. Includes the channel-report element in beacons and probe responses                                                                                                                                 |
| neighbor-report {hybrid}   | Optional. Enables responding to neighbor-report requests <ul style="list-style-type: none"><li>• hybrid - Optional. Uses the hybrid model of smart-rf neighbors and roaming frequency to neighbors</li></ul> |

#### Examples

```
rfs4000-229D58(config-wlan-test)#radio-resource-measurement
rfs4000-229D58(config-wlan-test)#show context
wlan test
 ssid test
 vlan 1
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 radio-resource-measurement
 controller-assisted-mobility
rfs4000-229D58(config-wlan-test)#
```

radius

Configures RADIUS related parameters

Supported in the following platforms:

- Access Points — AP 6522, AP 6532, AP 6562, AP 7502, AP 7522, AP 7532, AP 7161, AP 81XX, AP 8232
- Wireless Controllers — RFS 4000, RFS 6000
- Service Platforms — NX 7500, NX 9500, NX 9510

#### Syntax

```
radius [dynamic-authorization|nas-identifier|nas-port-id|vlan-assignment]
radius [dynamic-authorization|nas-identifier <NAS-ID>|nas-port-id <NAS-PORT-ID>|
 vlan-assignment]
```

## Parameters

`radius [dynamic-authorization|nas-identifier <NAS-ID>|nas-port-id <NAS-PORT-ID>|vlan-assignment]`

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dynamic-authorization     | Enables support for disconnect and change of authorization messages (RFC5176). When enabled, this option extends the RADIUS protocol to support unsolicited messages from the RADIUS server. These messages allow administrators to issue CoA (change of authorization) messages, which affect session authorization, or DM (disconnect messages) that terminate a session immediately. This option is disabled by default.                                                                                                                                                                                                                                                                                                                                                                                            |
| nas-identifier <NAS-ID>   | Configures the NAS (network access server) identifier attribute, a value that identifies the access point or controller where the RADIUS messages originate. The value specified here is included in the RADIUS NAS-Identifier field for WLAN authentication and accounting packets. <ul style="list-style-type: none"><li>• &lt;NAS-ID&gt; - Specify the NAS identifier attribute (should not exceed 256 characters in length).</li></ul>                                                                                                                                                                                                                                                                                                                                                                             |
| nas-port-id <NAS-PORT-ID> | Configures the WLAN NAS port ID sent to the RADIUS server. The NAS port identifier should not exceed 256 characters. <ul style="list-style-type: none"><li>• &lt;NAS-PORT-ID&gt; - Specify the NAS port ID attribute (should not exceed 256 characters in length).</li></ul> <p>The profile database on the RADIUS server consists of user profiles for each connected NAS port. Each profile is matched to a username representing a physical port. When authorizing users, it queries the user profile database using a username representative of the physical NAS port making the connection. Set the numeric port value from 0 - 4294967295.</p>                                                                                                                                                                  |
| vlan-assignment           | Configures the VLAN assignment of a WLAN. RADIUS VLAN assignment is disabled by default. When enabled, this option assigns clients to the RADIUS server specified VLANs, overriding the WLAN configuration. This option is disabled by default. If, as part of the authentication process, the RADIUS server returns a client's VLAN-ID in a RADIUS access-accept packet, and this feature is enabled, all client traffic is forwarded on that VLAN. If disabled, the RADIUS server returned VLAN-ID is ignored and the VLAN specified using the <code>vlan/vlan-pool-member</code> options (in the WLAN config mode) is used. <p>If both the RADIUS VLAN assignment and the post authentication VLAN options are enabled, then RADIUS VLAN assignment takes priority over post authentication VLAN configuration.</p> |

## Examples

```
nx9500-6C8809(config-wlan-test)#radius vlan-assignment
nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type none
 protected-mgmt-frames mandatory
 radius vlan-assignment
 wing-extensions wmm-load-information
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 --More--
nx9500-6C8809(config-wlan-test)#
```

## Related Commands

|                 |                                                                                                                                                                                                                                                                           |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>no</code> | Disables support for disconnect and change of authorization messages. Disables the use of VLAN information received in RADIUS server responses, instead uses the VLAN provided in the WLAN configuration. Removes the NAS identifier and NAS port identifiers configured. |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

registration

Configures settings enabling dynamic registration and validation of devices by their MAC addresses. When configured, this option registers a device's MAC address, and allows direct access to a previously registered device.

This command also configures the external guest registration and validation server details. If using an external server to perform guest registration, authentication and accounting, use this command to configure the external server's IP address/hostname. When configured, access points and controllers forward guest registration requests to the specified registration server. In case of EGuest deployment, this external resource should point to the EGuest registration server.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
registration [device|device-OTP|external|user]
registration [device|device-OTP|user] group-name <RAD-GROUP-NAME> {agreement-refresh
<0-144000>|
expiry-time <1-43800>}
registration external [follow-aaa|host]
registration external follow-aaa {send-mode [http|https|udp]}
registration external host <IP/HOSTNAME> {proxy-mode |send-mode}
registration external host <IP/HOSTNAME> {proxy-mode [none|through-controller|
through-rf-domain-manager|through-centralized-controller]|send-mode [https|https|udp]}
```

#### Parameters

```
registration external follow-aaa {send-mode [http|https|udp]}
```

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| registration                | Enables dynamic guest-user registration and validation. This option is disabled by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| external                    | Specifies that the guest registration is handled by an external resource. Access points/controllers send registration requests to the external registration server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| follow-aaa                  | Uses an AAA policy to point to the guest registration, authentication, and accounting server. When used, guest registration is handled by the RADIUS server specified in the AAA policy used in the WLAN context.<br>In case of EGuest deployment, the RADIUS authentication and accounting server configuration in the AAA policy should point to the EGuest server. The use of 'follow-aaa' option is recommended in EGuest replica-set deployments.<br>For more information on enabling the EGuest server, see <a href="#">eguest-server (VX9000 only)</a> on page 990 (profile config mode).<br>For more information on configuring an EGuest deployment, see <a href="#">configuring ExtremeGuest captive-portal</a> . |
| send-mode [https https udp] | Optional. Specifies the protocol used to forward registration requests to the external AAA policy servers. The options are: <ul style="list-style-type: none"> <li>• HTTPS – Sends registration requests as HTTPS packet</li> <li>• HTTP – Sends registration requests as HTTP packet</li> <li>• UDP – Sends registration requests as UDP packet, using the UDP port 12322. This is the default setting.</li> </ul>                                                                                                                                                                                                                                                                                                         |

```
registration external host <IP/HOSTNAME> {proxy-mode [none|through-controller|
through-rf-domain-manager|through-centralized-controller]|send-mode [https|https|udp]}
```

|                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| registration                                                                                    | Configures dynamic guest registration and validation parameters. This option is disabled by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| external                                                                                        | Specifies that the guest registration is handled by an external resource. Access points/controllers send registration requests to the external registration server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| host <IP/HOSTNAME>                                                                              | Specifies the external registration server's IP address or hostname. When configured, access points/ controllers forward guest registration requests to the external registration server specified here.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| proxy-mode {none  through-controller  through-rf-domain-manager through-centralized-controller} | <p>Optional. Specifies the proxy mode. If a proxy is needed for connection, specify the proxy mode as through-controller, through-rf-domain. If no proxy is needed, select none.</p> <ul style="list-style-type: none"> <li>• none – Optional. Requests are sent directly to the controller from the requesting device</li> <li>• through-controller – Optional. Requests are proxied through the controller configuring the device</li> <li>• through-rf-domain-manager – Optional. Requests are proxied through the local RF Domain manager</li> <li>• through-centralized-controller – Optional. Requests are proxied through one of the controllers in a cluster, operating as the designated forwarder. Select this option if capture and redirection is on a cluster of wireless controller/ service platforms managing dependent/independent access points when redundancy is required.</li> </ul> <p>After specifying the proxy-mode, optionally specify the protocol used to send the requests to the external registration server host.</p> |
| send-mode [https https udp]                                                                     | <p>Optional. Specifies the communication protocol used. The options are;</p> <ul style="list-style-type: none"> <li>• HTTPS – Sends registration requests as HTTPS packets</li> <li>• HTTP – Sends registration requests as HTTP packets</li> <li>• UDP – Sends registration requests as UDP packet, using the UPD port 12322. This is the default setting.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

```
registration [device|device-OTP|user] group-name <RAD-GROUP-NAME>
{agreement-refresh <0-14400>|expiry-time <1-43800>}
```

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| registration              | Configures dynamic guest registration and validation parameters. This option is disabled by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| [device device-OTP  user] | <p>Configures the mode used to register guest users of this WLAN. Options include device, external, user, and device-OTP</p> <ul style="list-style-type: none"> <li>• device-OTP – Registers a device by its MAC address. During registration, the user, using the registered device, has to provide the e-mail address, mobile number, or member id, and the OTP (one-time-passcode) sent to the registered e-mail id or mobile number to complete registration. On subsequent logins, the user has to enter the OTP. If the MAC address of the device attempting login and the OTP combination matches, the user is allowed access. If using this option, set the WLAN authentication type as MAC authentication.</li> <li>• device – Registers a device by its MAC address. On subsequent logins, already registered MAC addresses are allowed access. If using this option, set the WLAN authentication type as <i>MAC authentication</i>.</li> <li>• user – Registers guest users using one of the following options: e-mail address, mobile-number, or member-id.</li> </ul> <p>If using any one of the above modes of registration, specify the RADIUS group to which the registered device or user is to be assigned post authentication.</p> |

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| group-name <RAD-GROUP-NAME>  | Configures the RADIUS group name to which registered users are associated. When left blank, users are not associated with a RADIUS group. <ul style="list-style-type: none"> <li>&lt;RAD-GROUP-NAME&gt; – Specify the RADIUS group name (should not exceed 64 characters).</li> </ul>                                                                                                                                                                                                |
| expiry-time <1-43800>        | Optional. Configures the amount of time, in hours, before registered addresses expire and must be re-entered <ul style="list-style-type: none"> <li>&lt;1-43800&gt; – Specify a value from 1 - 43800 hrs. The default is 1500 hrs.</li> </ul>                                                                                                                                                                                                                                        |
| agreement-refresh <0-144000> | Optional. Sets the time, in minutes, after which an inactive user has to refresh the WLAN's terms of agreement. For example, if the agreement refresh period is set to 1440 minutes, a user, who has been inactive for more than 1440 minutes (1 day) is served the agreement page, and is allowed access only after refreshing the terms of agreement. <ul style="list-style-type: none"> <li>&lt;0-100&gt; – Specify a value from 0 - 144000. The default is 0 minutes.</li> </ul> |

### Examples

```

nx9500-6C8809(config-wlan-test)#registration user group-name guest agreement-ref
resh 14400 expiry-time 2000
nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type none
 registration user group-name guest expiry-time 2000 agreement-refresh 14400
nx9500-6C8809(config-wlan-test)#

```

### Related Commands

|    |                                                                                                                                               |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------|
| no | Disables dynamic user registration and removes associated configurations. Also disables forwarding of user information to an external device. |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------|

## relay-agent

Enables support for DHCP/DHCPv6 relay agent information (option 82 and DHCPv6-LDRA) feature on this WLAN. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
relay-agent [dhcp-option82|dhcpv6-ldra]
```

### Parameters

```
relay-agent [dhcp-option82|dhcpv6-ldra]
```

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| relay-agent   | Enables support for the following DHCP and DHCPv6 options: option 82 and LDRA (Lightweight DHCPv6 Relay Agent) respectively. When enabled, this feature allows the DHCP/DHCPv6 relay agent to insert the relay agent information option (option 82, LDRA) in client requests forwarded to the DHCP/DHCPv6 server. This information provides the following: <ul style="list-style-type: none"> <li>• circuit ID suboption – Provides the SNMP port interface index</li> <li>• remote ID – Provides the controller’s MAC address</li> </ul> |
| dhcp-option82 | Enables DHCP option 82. DHCP option 82 provides client physical attachment information. This option is disabled by default.                                                                                                                                                                                                                                                                                                                                                                                                               |
| dhcpv6-ldra   | Enables the DHCPv6 relay agent. The LDRA feature allows DHCPv6 messages to be transmitted on existing networks that do not currently support IPv6 or DHCPv6. This option is disabled by default.                                                                                                                                                                                                                                                                                                                                          |

### Examples

```
rfs4000-229D58(config-wlan-test)#relay-agent dhcp-option82
rfs4000-229D58(config-wlan-test)#show context
wlan test
 ssid test
 vlan 1
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 radio-resource-measurement
 relay-agent dhcp-option82
 controller-assisted-mobility
rfs4000-229D58(config-wlan-test)#
nx9500-6C8809(config-wlan-test)#relay-agent dhcpv6-ldra
nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 relay-agent dhcpv6-ldra
nx9500-6C8809(config-wlan-test)#
```

### Related Commands

|           |                                                                                                           |
|-----------|-----------------------------------------------------------------------------------------------------------|
| <b>no</b> | Disables support for DHCP/DHCPv6 relay agent information (option 82 and DHCPv6-LDRA) feature on this WLAN |
|-----------|-----------------------------------------------------------------------------------------------------------|

### service (wlan-config-context)

Invokes service commands applicable in the WLAN configuration mode

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
service [allow-ht-only|allow-open-passpoint|client-load-balancing|cred-cache|eap-mac-mode|
eap-mac-multicopy|eap-mac-multikeys|eap-throttle|enforce-pmkid-validation|key-index|
monitor|
radio-crypto|reauthentication|session-timeout|tx-death-on-roam-detection|unresponsive-
```



```

client|
wpa-wpa2|show]
service [allow-ht-only|allow-open-passpoint|cred-cache [clear-on-4way-timeout|clear-on-
disconnect]]|
eap-mac-multicopy|eap-mac-multikeys|enforce-pmkid-validation|radio-crypto|reauthentication
seamless|
session-timeout mac|tx-deauth-on-roam-detection|show cli]
service eap-mac-mode [mac-always|normal]
service eap-throttle <0-254>
service key-index eap-wep-unicast <1-4>
service monitor [aaa-server|adoption|captive-portal|dhcp|dns]
service monitor [aaa-server|adoption vlan <1-4094>|captive-portal external-server]
service monitor [dhcp|dns] crm <RESOURCE-NAME> vlan <1-4094>
service unresponsive-client [attempts <1-1000>|ps-detect {threshold <1-1000>}|timeout
<1-60>]
service wpa-wpa2 exclude-ccmp

```

### Parameters

```

service [allow-ht-only|allow-open-passpoint|cred-cache [clear-on-4way-timeout|
clear-on-disconnect]]|eap-mac-multicopy|eap-mac-multikeys|enforce-pmkid-validation|radio-
crypto|
reauthentication seamless|session-timeout mac|tx-deauth-on-roam-detection|show cli]

```

|                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| allow-ht-only                                          | Only allows clients capable of High Throughput (802.11n) data rates to associate. This option is disabled by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| allow-open-passpoint                                   | Enables non-WPA2 security for passpoint WLANs. This option is disabled by default. For more information on passpoint policy and configuration, see <a href="#">PASSPOINT-POLICY</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| cred-cache [clear-on-4way-timeout clear-on-disconnect] | <p>Clears credential cache based on the parameter passed</p> <ul style="list-style-type: none"> <li>clear-on-4way-timeout – Clears cached client credentials after the 4way handshake with a client has timed out. This option is enabled by default.</li> <li>clear-on-disconnect – Clears cached client credentials after the client has disconnected from the network. This option is disabled by default.</li> </ul>                                                                                                                                                                                                                                                                                                 |
| eap-mac-multicopy                                      | Enables sending of multiple copies of broadcast and unicast messages. This option is disabled by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| eap-mac-multikeys                                      | Enables configuration of different key indices for MAC authentication. This option is disabled by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| enforce-pmkid-validation                               | <p>Validates the Predictive real-time PMKID (pairwise master key identifier) contained in a client's association request against the one present in the wpa-wpa2 handshake. This option is enabled by default.</p> <p>This functionality is based on the PKC (Proactive Key Caching) extension of the 802.11i EEEE standard. Whenever a wireless client successfully authenticates with a AP it receives a PMK (pairwise master key). PKC allows clients to cache this PMK and reuse it for future re-authentications with the same AP. The PMK is unique for every client and is identified by the PMKID. The PMKID is a combination of the hash of the PMK, a string, the station and the MAC addresses of the AP.</p> |
| radio-crypto                                           | Uses radio hardware for encryption and decryption. This is applicable only for devices using CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) encryption mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| reauthentication seamless                              | Enables seamless EAP client reauthentication without disconnecting client after the session has timed out. This option is enabled by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| session-timeout mac                                    | Enables reauthentication of MAC authenticated clients without disconnecting client after the session has timed out. This option is enabled by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

|                             |                                                                                                                                                            |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| tx-deauth-on-roam-detection | Transmits a de-authentication on the air while disassociating a client because its roam is detected on the wired side. This option is disabled by default. |
| show cli                    | Displays the CLI tree of the current mode. When used in the WLAN mode, this command displays the WLAN CLI structure.                                       |

`service eap-mac-mode [mac-always|normal]`

|              |                                                                                                                                                                                                                                                                          |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| eap-mac-mode | Configures the EAP and/or MAC authentication mode used with this WLAN. This option is enabled by default.                                                                                                                                                                |
| mac-always   | Enables both EAP and MAC authentication. MAC authentication is performed first, followed by EAP authentication. Clients are granted access based on the EAP authentication result. If a client does not have EAP, the MAC authentication result is used to grant access. |
| normal       | Grants client access if the client clears either EAP or MAC authentication. This is the default setting.                                                                                                                                                                 |

`service eap-throttle <0-254>`

|                      |                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| eap-throttle <0-254> | Enables EAP request throttling. Use this command to specify the maximum number of parallel EAP sessions allowed on this WLAN. Once this specified value is exceeded, all incoming EAP session requests are throttled. This option is enabled by default. <ul style="list-style-type: none"> <li>• &lt;0-254&gt; - Specify a value from 0 - 254. This default value is 0.</li> </ul> |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

`service key-index eap-wep-unicast <1-4>`

|                                 |                                                                                                                                                                                                                               |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| key-index eap-wep-unicast <1-4> | Configures an index with each key during EAP authentication with WEP. This option is enabled by default. <ul style="list-style-type: none"> <li>• &lt;1-4&gt; - Select a index from 1 - 4. The default value is 1.</li> </ul> |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

`service wpa-wpa2 exclude-ccmp`

|                       |                                                                                                                                                                                                                      |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wpa-wpa2 exclude-ccmp | Configures exclusion of CCMP requests when the authentication mode is set to tkip-ccmp. When enabled, it provides compatibility for client devices not compliant with tkip-ccmp. This option is disabled by default. |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

`service monitor [aaa-server|adoption vlan <1-4094>|captive-portal external-server]`

|            |                                                                                                                                                                                                                                                                                                                                                         |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| monitor    | Enables critical resource monitoring. In a WLAN, service monitoring enables regular monitoring of external AAA servers, captive portal servers, access point adoption, DHCP and DNS servers. When enabled, it allows administrators to notify users of a service's availability and make resource substitutions in case of unavailability of a service. |
| aaa-server | Enables external AAA server failure monitoring. When enabled monitors an external RADIUS server resource's AAA activity and ensures its adoption and availability. This feature is disabled by default.                                                                                                                                                 |

|                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| adoption<br>vlan<br><1-4094>              | <p>Enables adoption failure monitoring on an adopted AP. Also configures a adoption failover VLAN. This feature is disabled by default.</p> <ul style="list-style-type: none"> <li>VLAN &lt;1-4094&gt; - Specify the VLAN on which clients are placed when the connectivity between the AAP and the controller is lost.</li> </ul> <p>Configure a DHCP pool and gateway for the failover VLAN. Ensure the DHCP server is running on the AP. Also ensure that the DHCP pool is configured to have less lease time.</p> <p>When this feature is enabled on a WLAN, it allows adopted APs to monitor their connectivity with the controller. If and when this connectivity is lost, all new clients are placed in the configured adoption failover VLAN. They are served an IP by the DHCP server running on the AP. In this situation if a client tries to access a Web URL, the AP redirects the client to a page stating that the service is down.</p> <p>When the AAP's link to the switch is restored, clients are placed back in the WLAN's configured VLAN, and are served an IP from the corresponding configured DHCP server (external or on the AP/controller).</p> |
| captive-<br>portal<br>external-<br>server | <p>Enables external captive portal server failure monitoring. When enabled, monitors externally hosted captive portal activity, and user access to the controller or service platform managed network. This feature is disabled by default.</p> <p>When enabled, this feature enables APs to display, to an externally located captive portal's user, the no-service page when the captive portal's server is not reachable.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

```
service monitor [dhcp|dns] crm <RESOURCE-NAME> vlan <1-4094>
```

|         |                                                                                                                                                                                                                                                                           |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| monitor | Enables DHCP and/or DNS server monitoring on this WLAN.                                                                                                                                                                                                                   |
| dhcp    | Enables monitoring of a specified DHCP server. When the connection to the DHCP server is lost, captive portal users automatically migrate to a pre-defined VLAN. The feature is disabled by default.<br>Use the <i>crm</i> keyword to specify the DHCP server to monitor. |
| dns     | Enables monitoring of a specified DNS server. When the connection to the DNS server is lost, captive portal users automatically migrate to a pre-defined VLAN. The feature is disabled by default.<br>Use the <i>crm</i> keyword to specify the DNS server to monitor.    |

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| crm <RESOURCE-NAME> | <p>This keyword is common to the 'dhcp' and 'dns' parameters.</p> <ul style="list-style-type: none"> <li>crm - Identifies the DHCP and/or DNS server to monitor</li> <li>&lt;RESOURCE-NAME&gt; - Specify the name of the DHCP or DNS server.</li> </ul> <p>Once enabled, the CRM server monitors the DHCP/DNS server and updates their status as 'up' or 'down' depending on the availability of the resource. When either of these resources is down the wireless client is mapped to the failover VLAN and served with the 'no-service' page through the access point.</p>                                                                                                                                                             |
| vlan <1-4094>       | <p>This keyword is common to the 'dhcp' and 'dns' parameters. After specifying the DHCP/DNS sever resource, specify the failover VLAN.</p> <ul style="list-style-type: none"> <li>VLAN &lt;1-4094&gt; - Configures the failover VLAN from 1 - 4094.</li> </ul> <p>When the DHCP server resource becomes unavailable, the device falls back to the VLAN defined here. This VLAN has a DHCP server configured that provides a pool of IP addresses with a lease time less than the main DHCP server.</p> <p>When this DNS server resource becomes unavailable, the device falls back to the VLAN defined here. This VLAN has a DNS server configured that provides DNS address resolution until the main DNS server becomes available.</p> |

```
service unresponsive-client [attempts <1-1000>|ps-detect {threshold <1-1000>}]
timeout <1-60>]
```

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| unresponsive                   | Configures handling of unresponsive clients                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| attempts <1-1000>              | <p>Configures the maximum number of successive packets that failed transmission</p> <ul style="list-style-type: none"> <li>&lt;1-1000&gt; - Specify a value from 1 - 1000. The default is 7.</li> </ul>                                                                                                                                                                                                                                                                                |
| ps-detect {threshold <1-1000>} | <p>Enables the detection of power-save mode clients, whose PS stats has not been updated on the AP. This option is enabled by default.</p> <ul style="list-style-type: none"> <li>threshold - Optional. Configures the threshold at which power-save client detection is triggered</li> <li>&lt;1-1000&gt; - Configures the number of successive unacknowledged packets received before power-save detection is triggered. Specify a value from 1 - 1000. The default is 3.</li> </ul> |
| timeout <1-60>                 | <p>Configures the interval, in seconds, for successive packets not acknowledged by the client</p> <ul style="list-style-type: none"> <li>&lt;1-60&gt; - Specify a value from 1 - 60 seconds. The default is 3 seconds.</li> </ul>                                                                                                                                                                                                                                                      |

### Examples

```
rfs4000-229D58(config-wlan-test)#service allow-ht-only
rfs4000-229D58(config-wlan-test)#service monitor aaa-server
rfs4000-229D58(config-wlan-test)#show context
wlan test
 ssid test
 vlan 1
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 service monitor aaa-server
 service allow-ht-only
 controller-assisted-mobility
rfs4000-229D58(config-wlan-test)#
```

### Related Commands

no

Removes or reverts to default WLAN settings configured using the 'service' command

## shutdown

Shuts down a WLAN

The auto shutdown mechanism helps regulate the availability of a WLAN based on an administrator defined access period. Use this feature to shut down a WLAN on specific days and hours and restrict periods when the WLAN traffic is either not desired or cannot be properly administrated. The normal practice is to shut down WLANs when there are no users on the network, such as after hours, weekends or holidays. This allows administrators more time to manage mission critical tasks since the WLAN's availability is automated.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
shutdown {on-critical-resource <CR-NAME>/on-meshpoint-loss/on-primary-port-link-loss/on-unadoption}
```

### Parameters

```
shutdown {on-critical-resource <CR-NAME>/on-meshpoint-loss/on-primary-port-link-loss/on-unadoption}
```

|                                |                                                                                                                                                                                                                                               |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| shutdown                       | Auto shuts down the WLAN when specified events occur. Disabled by default.                                                                                                                                                                    |
| on-critical-resource <CR-NAME> | Optional. Auto shuts down the WLAN when critical resource failure occurs. Disabled by default. <ul style="list-style-type: none"><li>• &lt;CR-NAME&gt; - Specifies the name of the critical resource being monitored for this WLAN.</li></ul> |
| on-meshpoint-loss              | Optional. Auto shuts down the WLAN when the root meshpoint link fails (is unreachable). Disabled by default.                                                                                                                                  |
| on-primary-port-link-loss      | Optional. Auto shuts down the WLAN when a device losses its primary Ethernet port (ge1/up1) link. Disabled by default.                                                                                                                        |
| on-unadoption                  | Optional. Auto shuts down the WLAN when an adopted device becomes unadopted. Disabled by default.                                                                                                                                             |

### Usage Guidelines

If the shutdown on-meshpoint-loss feature is enabled, the WLAN status changes only if the meshpoint and the WLAN are mapped to the same VLAN. If the meshpoint is mapped to VLAN 1 and the WLAN is mapped to VLAN 2, then the WLAN status does not change on loss of the meshpoint.

### Examples

```
nx9500-6C8809(config-wlan-test)#shutdown on-unadoption
<exsw1>(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type none
```

```

protected-mgmt-frames mandatory
radius vlan-assignment
wing-extensions wmm-load-information
client-load-balancing probe-req-intvl 5ghz 5
client-load-balancing band-discovery-intvl 2
acl exceed-rate wireless-client-denied-traffic 20 disassociate
proxy-arp-mode strict
broadcast-dhcp validate-offer
shutdown on-unadoption
http-analyze controller
nx9500-6C8809(config-wlan-test)#

```

#### Related Commands

|           |                                                                                                                                                                                                                                                        |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>no</b> | Disables auto shut down WLAN. Use the optional keywords provided to disable auto shut down of the WLAN upon critical resource failure, when meshpoint links fail, when the primary Ethernet port (e1/up1) loses link, or when the WLAN gets unadopted. |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### ssid

Configures a WLAN's SSID

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
ssid <SSID>
```

#### Parameters

```
ssid <SSID>
```

|                                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------|
| <SSID> Specify the WLAN's SSID. The WLAN SSID is case sensitive and alphanumeric. It's length should not exceed 32 characters. |
|--------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```

nx9500-6C8809(config-wlan-test)#ssid testWLAN1
nx9500-6C8809(config-wlan-test)#show context
wlan test
ssid testWLAN1
bridging-mode local
encryption-type none
authentication-type none
protected-mgmt-frames mandatory
radius vlan-assignment
wing-extensions wmm-load-information
client-load-balancing probe-req-intvl 5ghz 5
client-load-balancing band-discovery-intvl 2
acl exceed-rate wireless-client-denied-traffic 20 disassociate
proxy-arp-mode strict
broadcast-dhcp validate-offer
shutdown on-unadoption
http-analyze controller
nx9500-6C8809(config-wlan-test)#

```

#### Related Commands

|           |                         |
|-----------|-------------------------|
| <b>no</b> | Removes the WLAN's SSID |
|-----------|-------------------------|

## t5-client-isolation

Disallows clients connecting to the WLAN to communicate with one another. This setting applies exclusively to CPE devices managed by a T5 controller and is disabled by default.

A T5 controller uses the IPX operating system to manage its connected radio devices, as opposed to the WiNG operating system used by RFS wireless controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The CPEs are the T5 controller managed radio devices using the IPX operating system. These CPEs use a DSL as their high speed Internet access mechanism using the CPE's physical wallplate connection and phone jack.



### Note

This setting is applicable only when this WLAN supports T5 controllers and their connected CPEs.

Supported in the following platforms:

- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

### Syntax

`t5-client-isolation`

### Parameters

None

### Examples

```
nx9500-6C8809(config-wlan-test)#t5-client-isolation
nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type none
 t5-client-isolation
nx9500-6C8809(config-wlan-test)#
```

### Related Commands

|                 |                                                                       |
|-----------------|-----------------------------------------------------------------------|
| <code>no</code> | Allows clients connecting to the WLAN to communicate with one another |
|-----------------|-----------------------------------------------------------------------|

## t5-security

Configures T5 PowerBroadband security settings

A T5 controller uses the IPX operating system to manage its connected radio devices, as opposed to the WiNG operating system used by RFS controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The CPEs are the T5 controller managed radio devices using the IPX operating system. These CPEs use DSL as their high speed Internet access mechanism using the CPE's physical wallplate connection and phone jack.



### Note

This setting is applicable only when this WLAN supports T5 controllers and their connected CPEs.

Supported in the following platforms:

- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

### Syntax

```
t5-security [static-wep|wpa-enterprise|wpa-personal]
t5-security static-wep encryption-type [wep128|wep64] [hex <STRING>|passphrase <STRING>]
t5-security [wpa-enterprise|wpa-personal] encryption-type [ccmp|tkip|tkip-ccmp]
version [mixed|wpa|wpa2]
```

### Parameters

```
t5-security static-wep encryption-type [wep128|wep64] [hex <STRING>|passphrase <STRING>]
```

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| t5-security static-wep         | Configures the T5 WLAN security type as static-wep                                                                                                                                                                                                                                                                                                                                                                                                                          |
| encryption-type [wep128 wep64] | Applies one of the following encryption algorithms to the T5 support WLAN configuration: WEP64 or WEP128                                                                                                                                                                                                                                                                                                                                                                    |
| hex <STRING>                   | Configures the hex password (used to derive the security key) <ul style="list-style-type: none"> <li>• &lt;STRING&gt; - Specify the hex password (should not exceed the 10 - 26 characters).</li> </ul>                                                                                                                                                                                                                                                                     |
| passphrase <STRING>            | Configures the passphrase shared by both transmitting and receiving authenticators <ul style="list-style-type: none"> <li>• &lt;STRING&gt; - Specify the passphrase. It could either be an alphanumeric string of 8 to 63 ASCII characters or 64 HEX characters. The alphanumeric string allows character spaces. This string is converted to a numeric value. Configuring a passphrase saves you the need to create a 256-bit key each time keys are generated.</li> </ul> |

```
t5-security [wpa-enterprise|wpa-personal] encryption-type [ccmp|tkip|tkip-ccmp]
version [mixed|wpa|wpa2]
```

|                                           |                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| t5-security [wpa-enterprise wpa-personal] | Configures the T5 WLAN security type as: wpa-enterprise OR wpa-personal                                                                                                                                                                                                                                                |
| encryption-type [ccmp tkip tkip-ccmp]     | The following parameters are common to the <i>wpa-enterprise</i> and <i>wpa-personal</i> keywords: <ul style="list-style-type: none"> <li>• [ccmp tkip tkip-ccmp] - Applies one of the following encryption algorithms to the T5 support WLAN configuration: <b>CCMP</b>, <b>TKIP</b>, or <b>TKIP-CCMP</b>.</li> </ul> |
| version [mixed wpa wpa2]                  | The following parameters are common to the <i>wpa-enterprise</i> and <i>wpa-personal</i> keywords: <ul style="list-style-type: none"> <li>• version - Applies one of the following encryption schemes to the T5 support WLAN configuration: <b>WPA</b>, <b>WPA2</b>, or <b>mixed</b>.</li> </ul>                       |

### Examples

```
nx9500-6C8809(config-wlan-test)#t5-security wpa-enterprise encryption-type ccmp version wpa
nx9500-6C8809(config-wlan-test)#show context
wlan test
ssid test
bridging-mode local
encryption-type none
authentication-type none
t5-security wpa-enterprise encryption-type ccmp version wpa
t5-client-isolation
nx9500-6C8809(config-wlan-test)#
```

### Related Commands

|    |                                                            |
|----|------------------------------------------------------------|
| no | Removes the configured T5 PowerBroadband security settings |
|----|------------------------------------------------------------|



## time-based-access

Configures time-based client access to the network resources. Use this feature to assign fixed days and time of WLAN access for wireless clients.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
time-based-access days [sunday|monday|tuesday|wednesday|thursday|friday|saturday|all|weekends|weekdays] {start <START-TIME>} [end <END-TIME>]
```

### Parameters

```
time-based-access days [sunday|monday|tuesday|wednesday|thursday|friday|saturday|all|weekends|weekdays] {start <START-TIME>} [end <END-TIME>]
```

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| day <option>       | Specifies the day or days on which the client can access the WLAN <ul style="list-style-type: none"><li>• sunday – Allows access on Sundays only</li><li>• monday – Allows access on Mondays only</li><li>• Tuesdays – Allows access on Tuesdays only</li><li>• wednesday – Allows access on Wednesdays only</li><li>• thursday – Allows access on Thursdays only</li><li>• friday – Allows access on Fridays only</li><li>• saturday – Allows access on Saturdays only</li><li>• weekends – Allows access on weekends only</li><li>• weekdays – Allows access on weekdays only</li><li>• all – Allows access on all days</li></ul> |
| start <START-TIME> | Optional. Specifies the access start time in hours and minutes (HH:MM)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| end <END-TIME>     | Specifies the access end time in hours and minutes (HH:MM)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

### Examples

```
nx9500-6C8809(config-wlan-test)#time-based-access days weekdays start 10:00 end 16:30
nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid testWLAN1
 bridging-mode local
 encryption-type none
 authentication-type none
 protected-mgmt-frames mandatory
 radius vlan-assignment
 time-based-access days weekdays start 10:00 end 16:30
 --More--
nx9500-6C8809(config-wlan-test)#
```

### Related Commands

|           |                                                   |
|-----------|---------------------------------------------------|
| <b>no</b> | Removes the configured time-based-access settings |
|-----------|---------------------------------------------------|

## use (wlan-config-mode)

This command associates an existing captive portal and other policies with a WLAN.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
use [aaa-policy|application-policy|association-acl-policy|bonjour-gw-discovery-policy|
captive-portal|ip-access-list|ipv6-access-list|mac-access-list|passpoint-policy|roaming-
assist-policy|
url-filter|wlan-qos-policy]
use [aaa-policy <AAA-POLICY-NAME>|application-policy <POLICY-NAME>|
association-acl-policy <ASSOCIATION-POLICY-NAME>|bonjour-gw-discovery-policy <POLICY-NAME>|
captive-portal <CAPTIVE-PORTAL-NAME>|passpoint-policy <PASSPOINT-POLICY-NAME>|
roaming-assist-policy <POLICY-NAME>|url-filter <URL-FILTER-NAME>|wlan-qos-policy <WLAN-QOS-
POLICY-NAME>]
use ip-access-list [in|out] <IP-ACCESS-LIST-NAME>
use ipv6-access-list [in|out] <IPv6-ACCESS-LIST-NAME>
use mac-access-list [in|out] <MAC-ACCESS-LIST-NAME>
```

### Parameters

```
use [aaa-policy <AAA-POLICY-NAME>|application-policy <POLICY-NAME>|
association-acl-policy <ASSOCIATION-POLICY-NAME>|bonjour-gw-discovery-policy <POLICY-NAME>|
captive-portal <CAPTIVE-PORTAL-NAME>|passpoint-policy <PASSPOINT-POLICY-NAME>|
roaming-assist-policy <POLICY-NAME>|url-filter <URL-FILTER-NAME>|wlan-qos-policy <WLAN-QoS-
POLICY-NAME>]
```

|                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| aaa-policy <AAA-POLICY-NAME>              | <p>Uses an existing AAA policy with a WLAN</p> <ul style="list-style-type: none"> <li>• &lt;AAA-POLICY-NAME&gt; - Specify the AAA policy name.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| application-policy <POLICY-NAME>          | <p>Uses an existing application policy with a WLAN. An application policy defines actions to perform on a packet when it matches a specified set of pre-defined applications or application categories.</p> <ul style="list-style-type: none"> <li>• &lt;POLICY-NAME&gt; - Specify the policy name.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                |
| association-acl <ASSOCIATION-POLICY-NAME> | <p>Uses an existing association ACL policy with a WLAN</p> <ul style="list-style-type: none"> <li>• &lt;ASSOCIATION-POLICY-NAME&gt; - Specify the association ACL policy name.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| bonjour-gw-discovery-policy <POLICY-NAME> | <p>Uses an existing Bonjour GW Discovery policy with a WLAN. When associated, the Bonjour GW Discovery policy defines a list of Apple services clients can discover across subnets.</p> <p>Bonjour enables discovery of services on a LAN. Bonjour allows the setting up a network (without any configuration) in which services such as printers, scanners and file-sharing servers can be found using Bonjour. Bonjour only works within a single broadcast domain. However, with a special DNS configuration, it can be extended to find services across broadcast domains.</p> <ul style="list-style-type: none"> <li>• &lt;POLICY-NAME&gt; - Specify the Bonjour GW Discovery policy name. Should be existing and configured.</li> </ul> |
| captive-portal <CAPTIVE-PORTAL-NAME>      | <p>Specifies the captive-portal policy to use if enforcing captive-portal authentication on this WLAN</p> <ul style="list-style-type: none"> <li>• &lt;CAPTIVE-PORTAL-NAME&gt; - Specify the captive-portal policy name. Should be existing and configured.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

|                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>passpoint-policy<br/>&lt;PASSPOINT-POLICY-NAME&gt;</p> | <p>Associates a passpoint policy (Hotspot2 configuration) with this WLAN.</p> <ul style="list-style-type: none"> <li>• &lt;PASSPOINT-POLICY-NAME&gt; – Specify the Passpoint policy name. Should be existing and configured.</li> </ul> <p>Map a passpoint policy to a WLAN. Since the configuration gets applied to the radio by BSS, only the Hotspot 2.0 configuration of primary WLANs on a BSSID is used. Incoming Hotspot 2.0 GAQ/ANQP requests from clients are identified by their destination MAC addresses and are handled by the passpoint policy from the primary WLAN on that BSS.</p> <p>Define one passpoint policy for every WLAN configured.</p> |
| <p>roaming-assist-policy<br/>&lt;POLICY-NAME&gt;</p>      | <p>Associates an existing roaming assist policy with this WLAN</p> <ul style="list-style-type: none"> <li>• &lt;POLICY-NAME&gt; – Specify the Roaming Assist policy name. Should be existing and configured.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <p>url-filter &lt;URL-FILTER-NAME&gt;</p>                 | <p>Associates an existing URL list with this WLAN</p> <ul style="list-style-type: none"> <li>• &lt;URL-FILTER-NAME&gt; – Specify the URL filter name. Should be existing and configured.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <p>wlan-qos-policy &lt;WLAN-QOS-POLICY-NAME&gt;</p>       | <p>Uses an existing WLAN QoS policy with a WLAN</p> <ul style="list-style-type: none"> <li>• &lt;wlan-qos-policy-name&gt; – Specify the WLAN QoS policy name. Should be existing and configured.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

`use ip-access-list [in|out] <IP-ACCESS-LIST-NAME>`

|                                                            |                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>ip-access-list [in out] &lt;IP-ACCESS-LIST-NAME&gt;</p> | <p>Applies an IP access list to incoming and outgoing packets</p> <ul style="list-style-type: none"> <li>• in – Applies the IP ACL to incoming packets</li> <li>• out – Applies IP ACL to outgoing packets</li> <li>• &lt;IP-ACCESS-LIST-NAME&gt; – Specify the IP access list name.</li> </ul> |
|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

`use ipv6-access-list [in|out] <IPv6-ACCESS-LIST-NAME>`

|                                                                |                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>ipv6-access-list [in out] &lt;IPv6-ACCESS-LIST-NAME&gt;</p> | <p>Applies an IPv6 access list to incoming and outgoing packets</p> <ul style="list-style-type: none"> <li>• in – Applies the IPv6 ACL to incoming packets</li> <li>• out – Applies IPv6 ACL to outgoing packets</li> <li>• &lt;IPv6-ACCESS-LIST-NAME&gt; – Specify the IPv6 access list name.</li> </ul> |
|----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

`use mac-access-list [in|out] <MAC-ACCESS-LIST-NAME>`

|                                                              |                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>mac-access-list [in out] &lt;MAC-ACCESS-LIST-NAME&gt;</p> | <p>Applies a MAC access list to incoming and outgoing packets.</p> <ul style="list-style-type: none"> <li>• in – Applies the MAC ACL to incoming packets</li> <li>• out – Applies MAC ACL to outgoing packets</li> <li>• &lt;MAC-ACCESS-LIST-NAME&gt; – Specify the MAC access list name.</li> </ul> |
|--------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Usage Guidelines

IP and MAC ACLs act as firewalls within a WLAN. WLANs use ACLs as firewalls to filter or mark packets based on the WLAN from which they arrive, as opposed to filtering packets on layer 2 ports. An ACL contains an ordered list of ACEs (Access Control Entries). Each ACE specifies a set of conditions (rules) and the action taken in case of a match. The action can be permit, deny, or mark. Therefore, when a packet matches an ACE's conditions, it is either forwarded, dropped, or marked depending on the

action specified in the ACE. The order of conditions in the list is critical since filtering is stopped after the first match.

IP ACLs contain deny and permit rules specifying source and destination IP addresses. Each rule has a precedence order assigned. Both IP and non-IP traffic on the same layer 2 interface can be filtered by applying both an IP ACL and a MAC.

Additionally, you can filter layer 2 traffic on a physical layer 2 interface using MAC addresses. A MAC firewall rule uses source and destination MAC addresses for matching operations, where the result is a typical allow, deny, or mark designation to WLAN packet traffic.

Keep in mind IP and non-IP traffic on the same layer 2 interface can be filtered by applying both an IP ACL and a MAC ACL to the interface.

#### Examples

```
nx9500-6C8809(config-wlan-test)#use aaa-policy test
<exsw1>(config-wlan-test)#use association-acl-policy test
nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid testWLAN1
 bridging-mode local
 encryption-type none
 authentication-type none
 protected-mgmt-frames mandatory
 radius vlan-assignment
 time-based-access days weekdays start 10:00 end 16:30
 wing-extensions wmm-load-information
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 use aaa-policy test
 use association-acl-policy test
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 proxy-arp-mode strict
 broadcast-dhcp validate-offer
 shutdown on-unadoption
 http-analyze controller
nx9500-6C8809(config-wlan-test)#
nx9500-6C8809(config-wlan-ipad_clients)#use bonjour-gw-discovery-policy generic
nx9500-6C8809(config-wlan-ipad_clients)#show context
wlan ipad_clients
 ssid ipad_clients
 vlan 41
 bridging-mode local
 encryption-type none
 authentication-type none
 use bonjour-gw-discovery-policy generic
nx9500-6C8809(config-wlan-ipad_clients)#
```

#### Related Commands

|    |                                                                                                                                                                                                                                                                                         |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| no | Removes the following policies associated with a WLAN: aaa-policy, application-policy, association-acl-policy, bonjour-gw-discovery-policy, captive-portal, ip-access-list, ipv6-access-list, mac-access-list, passpoint-policy, roaming-assist-policy, url-filter, or wlan-qos-policy. |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

vlan

Sets the VLAN where traffic from this WLAN is mapped

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
vlan [<1-4094>|<VLAN-ALIAS-NAME>]
```

### Parameters

```
vlan [<1-4094>|<VLAN-ALIAS-NAME>]
```

|                   |                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-4094>          | Sets a WLAN's VLAN ID. This command starts a new VLAN assignment for a WLAN index. All prior VLAN settings are erased.<br>Use this command to assign just one VLAN to the WLAN. Utilizing a single VLAN per WLAN is a more typical deployment scenario than using a VLAN pool.                                                                                    |
| <VLAN-ALIAS-NAME> | Assigns a VLAN alias to the WLAN. The VLAN alias should be pre-existing and configured. A VLAN alias maps a name to a VLAN ID. When applied to ports (for example GE ports) using the trunk mode, a VLAN alias denies or permits traffic, on the port, to and from the VLANs specified in the alias. For more information on aliases, see <a href="#">alias</a> . |

### Examples

```
nx9500-6C8809(config-wlan-test)#vlan 4
nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid testWLAN1
 vlan 4
 bridging-mode local
 encryption-type none
 authentication-type none
 protected-mgmt-frames mandatory
 radius vlan-assignment
 time-based-access days weekdays start 10:00 end 16:30
 wing-extensions wmm-load-information
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 use aaa-policy test
 use association-acl-policy test
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 proxy-arp-mode strict
 broadcast-dhcp validate-offer
 shutdown on-unadoption
 http-analyze controller
nx9500-6C8809(config-wlan-test)#
```

### Related Commands

|           |                                       |
|-----------|---------------------------------------|
| <b>no</b> | Removes a WLAN's default VLAN mapping |
|-----------|---------------------------------------|

### vlan-pool-member

Adds a member VLAN to a WLAN's VLAN pool. Use this option to define the VLANs available to this WLAN. Additionally, define the number of wireless clients supported by each VLAN.



#### Note

Configuration of a VLAN pool overrides the 'vlan' configuration.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
vlan-pool-member <WORD> {limit <0-8192>}
```

#### Parameters

```
vlan-pool-member <WORD> {limit <0-8192>}
```

|                  |                                                                                                                                                                                                                              |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vlan-pool-member | Adds a member VLAN to a WLAN's VLAN pool<br>Since users belonging to separate VLANs can share the same WLAN, it is not necessary to create a new WLAN for every VLAN in the network.                                         |
| <WORD>           | Define the VLANs available to this WLAN. It is either a single index, or a list of VLAN IDs (for example, 1,3,7), or a range (for example, 1-10)                                                                             |
| limit <0-8192>   | Optional. Is ignored if the number of clients are limited and well within the limits of the DHCP pool on the VLAN <ul style="list-style-type: none"> <li>• &lt;0-8192&gt; - Specifies the number of users allowed</li> </ul> |

#### Examples

```
nx9500-6C8809(config-wlan-test)#vlan-pool-member 1-10 limit 1
nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid testWLAN1
 vlan-pool-member 1 limit 1
 vlan-pool-member 2 limit 1
 vlan-pool-member 3 limit 1
 vlan-pool-member 4 limit 1
 vlan-pool-member 5 limit 1
 vlan-pool-member 6 limit 1
 vlan-pool-member 7 limit 1
 vlan-pool-member 8 limit 1
 vlan-pool-member 9 limit 1
 vlan-pool-member 10 limit 1
 bridging-mode local
 encryption-type none
 authentication-type none
 protected-mgmt-frames mandatory
 radius vlan-assignment
 time-based-access days weekdays start 10:00 end 16:30
--More--
nx9500-6C8809(config-wlan-test)#
```

#### Related Commands

|    |                                            |
|----|--------------------------------------------|
| no | Removes the list of VLANs mapped to a WLAN |
|----|--------------------------------------------|

#### wep128

Configures WEP128 parameters

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000

- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
wep128 [key|keys-from-passkey|transmit-key]
wep128 key <1-4> [ascii|hex] [0 <WORD>|2 <WORD>|<WORD>]
wep128 keys-from-passkey <WORD>
wep128 transmit-key <1-4>
```

### Parameters

```
wep128 key <1-4> [ascii|hex] [0 <WORD>|2 <WORD>|<WORD>]
```

|                                  |                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wep128                           | Configures WEP128 parameters. The parameters are: key, key-from-passkey, and transmit-key.                                                                                                                                                                                                                                                            |
| key <1-4>                        | Use to configure the key number <ul style="list-style-type: none"> <li>• &lt;1-4&gt; – Specify the key number from 1 - 4.</li> </ul>                                                                                                                                                                                                                  |
| ascii [0 <WORD> 2 <WORD> <WORD>] | Sets keys as ASCII characters (5 characters for WEP64, 13 for WEP128) <ul style="list-style-type: none"> <li>• 0 &lt;WORD&gt; – Configures a clear text key</li> <li>• 2 &lt;WORD&gt; – Configures an encrypted key</li> <li>• &lt;WORD&gt; – Configures keys as 13 ASCII characters converted to hex, or 26 hexadecimal characters</li> </ul>        |
| hex [0 <WORD> 2 <WORD> <WORD>]   | Sets keys as hexadecimal characters (10 characters for WEP64, 26 for WEP128) <ul style="list-style-type: none"> <li>• 0 &lt;WORD&gt; – Configures a clear text key</li> <li>• 2 &lt;WORD&gt; – Configures an encrypted key</li> <li>• &lt;WORD&gt; – Configures keys as 13 ASCII characters converted to hex, or 26 hexadecimal characters</li> </ul> |

```
wep128 keys-from-passkey <WORD>
```

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| keys-from-passkey <WORD> | Specifies a pass key. The pass key can be any alphanumeric string. Controllers, service platforms, Access Points and their connected clients use the algorithm to convert an ASCII string to the same hexadecimal number. Clients without adapters need to use WEP keys manually configured as hexadecimal numbers. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify a pass key from 4 - 32 characters.</li> </ul> |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
wep128 transmit-key <1-4>
```

|                    |                                                                                                                                                                                                      |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| transmit-key <1-4> | Configures the key index used for transmission from an AP to a wireless client or service platform <ul style="list-style-type: none"> <li>• &lt;1-4&gt; – Specify a key index from 1 - 4.</li> </ul> |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
NOC-NX9500(config-wlan-test)#wep128 key 1 ascii 123456789abcd
NOC-NX9500(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type none
 wep128 key 1 hex 0 31323334353637383961626364
NOC-NX9500(config-wlan-test)#
```

### Related Commands

no

Resets the WEP128 parameters to factory-default values.

## wep64

Configures WEP64 parameters

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
wep64 [key|keys-from-passkey|transmit-key]
wep64 key <1-4> [ascii|hex] [0 <WORD>|2 <WORD>|<WORD>]
wep64 keys-from-passkey <WORD>
wep64 transmit-key <1-4>
```

### Parameters

```
wep64 key <1-4> [ascii|hex] [0 <WORD>|2 <WORD>|<WORD>]
```

|                                          |                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wep64                                    | Configures WEP64 parameters<br>The parameters are: key, key-from-passkey, and transmit-key.                                                                                                                                                                                                                                                                       |
| key <1-4>]                               | Configures pre-shared hex keys <ul style="list-style-type: none"><li>• &lt;1-4&gt; – Configures a maximum of four key indexes. Select a key index from 1 - 4.</li></ul>                                                                                                                                                                                           |
| ascii [0 <WORD>] 2<br><WORD>]<br><WORD>] | Sets keys as ASCII characters (5 characters for WEP64, 13 for WEP128) <ul style="list-style-type: none"><li>• 0 &lt;WORD&gt; – Configures a clear text key</li><li>• 2 &lt;WORD&gt; – Configures an encrypted key</li><li>• &lt;WORD&gt; – Configures key (10 hex or 5 ASCII characters for WEP64, 26 hex or 13 ASCII characters for WEP128).</li></ul>           |
| hex [0 <WORD>] 2<br><WORD>]<br><WORD>]   | Sets keys as hexadecimal characters (10 characters for WEP64, 26 for WEP128) <ul style="list-style-type: none"><li>• 0 &lt;WORD&gt; – Configures a clear text key</li><li>• 2 &lt;WORD&gt; – Configures an encrypted key</li><li>• &lt;WORD&gt; – Configures the key (10 hex or 5 ASCII characters for WEP64, 26 hex or 13 ASCII characters for WEP128)</li></ul> |

```
wep64 keys-from-passkey <WORD>
```

|                          |                                                                                                                                                              |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| keys-from-passkey <WORD> | Specifies a pass key from which keys are derived <ul style="list-style-type: none"><li>• &lt;WORD&gt; – Specify a pass key from 4 - 32 characters.</li></ul> |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
wep64 transmit-key <1-4>
```

|                    |                                                                                                                                                                                                    |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| transmit-key <1-4> | Configures the key index used for transmission from an AP to a wireless client or service platform <ul style="list-style-type: none"><li>• &lt;1-4&gt; – Specify a key index from 1 - 4.</li></ul> |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



## Examples

```
NOC-NX9500(config-wlan-test2)#wep64 key 1 hex 1CBF427D50
NOC-NX9500(config-wlan-test2)#wep64 transmit-key 1
NOC-NX9500(config-wlan-test2)#show context
wlan test2
 ssid test2
 bridging-mode local
 encryption-type none
 authentication-type none
 wep64 key 1 hex 0 1CBF427D50
NOC-NX9500(config-wlan-test2)#
```

## Related Commands

|           |                                                       |
|-----------|-------------------------------------------------------|
| <b>no</b> | Resets the WEP64 parameters to factory-default values |
|-----------|-------------------------------------------------------|

## wing-extensions

Enables support for WiNG-specific client extensions to the IEEE 802.11x WLAN standards that potentially increase client roaming reliability and handshake speed

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
wing-extensions [ap-attributes-information {include-hostname}|
coverage-hole-detection {11k-clients/offset <5-20>/threshold <-80--60>}|
ft-over-ds-aggregate|move-command|scan-assist {channel-info-interval <6-9>}|
smart-scan|wing-load-information|wmm-load-information]
```

## Parameters

```
wing-extensions [ap-attributes-information {include-hostname}|
coverage-hole-detection {11k-clients/offset <5-20>/threshold <-80--60>}|
ft-over-ds-aggregate|move-command|scan-assist {channel-info-interval <6-9>}|
smart-scan|wing-load-information|wmm-load-information]
```

|                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wing-extensions                              | Enables support for inclusion of WiNG-specific client extensions in radio transmissions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| ap-attributes-information {include-hostname} | <p>Enables support for AP attributes IE (information element)</p> <ul style="list-style-type: none"><li>• include-hostname - Optional. When enabled, includes AP's hostname, as a sub-element, in the AP attributes IE.</li></ul> <p>The AP attributes IE is vendor-specific and, when enabled, is added to beacons and probe responses. Inclusion of AP attributes IE allows Extreme Networks terminals to:</p> <ul style="list-style-type: none"><li>• - Recognize Extreme APs</li><li>• - Determine if the AP supports PAN BU features, irrespective of whether these features are enabled or not.</li></ul> <p>AP attributes IE is not added to beacons and probe responses by default.</p> |

|                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>verage-hole-detection {11k-clients  offset &lt;5-20&gt;  threshold &lt;-80--60&gt;}</p> | <p>Enables CHD (coverage hole detection) and configures CHD parameters. When enabled, allows clients (MUs) to inform an access point when it experiences a coverage hole. A coverage hole is an area of poor wireless coverage not supported by a WiNG managed access point radio. Enable radio resource measurement prior to enabling CHD. For enabling radio resource measurement, see <a href="#">radio-resource-measurement</a>. CHD is disabled by default.</p> <p>After enabling CHD, optionally configure the following parameters:</p> <ul style="list-style-type: none"> <li>• 11k-clients - Optional. Provides coverage hole detection to 802.11k-only-capable clients. This is a reduced set of coverage hole detection capabilities (standard 11k messages and behaviors). This option is disabled by default.</li> <li>• offset &lt;5-20&gt; - Optional. Configures the offset added to the threshold to obtain the access point's signal strength (as seen by the client) considered adequate. <ul style="list-style-type: none"> <li>• &lt;5-20&gt; - Specify the offset value from 5 - 20. The default is 5.</li> </ul> </li> <li>• threshold - Optional. Configures the access point's signal strength threshold. When Radio Resource Measurement and CVG Hole are enabled, specify a threshold for the AP's signal strength (as seen by the client) below which a coverage hole incident is reported by the client. <ul style="list-style-type: none"> <li>• &lt;-80--60&gt; - Specify the threshold from -80 - -60 dBm. The default is -70 dBm.</li> </ul> </li> </ul> |
| <p>ft-over-ds-aggregate</p>                                                                | <p>Enables FT (fast-transition) aggregation of action frames. When enabled, increases roaming speed by eliminating separate key exchange handshake frames with potential roam candidates. Enable fast transition to complete an initial FT over DS (distribution system) handshake with multiple roam candidates (up to 6) at once, eliminating the need to send separate FT over DS handshakes to each roam candidate. This option is disabled by default.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <p>move-command</p>                                                                        | <p>Enables use of HFSR (Hyper Fast Secure Roaming) for clients on this WLAN. This feature applies only to certain client devices. This option is disabled by default.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <p>scan-assist {channel-info-interval &lt;6-9&gt;}</p>                                     | <p>Enables support for scanning assist. When enabled, allows faster roams on DFS (Dynamic Frequency Selection) channels by eliminating passive scans. Clients get channel information directly from possible roam candidates. This option is disabled by default.</p> <ul style="list-style-type: none"> <li>• channel-info-interval &lt;6-9&gt; - Optional. Configures the interval at which channel information is periodically retrieved from potential roam candidates without requesting scan assist. <ul style="list-style-type: none"> <li>• &lt;6-9&gt; - Specify the interval from 6 - 9 seconds. When enabled, the default value is 8 seconds.</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <p>smart-scan</p>                                                                          | <p>Enables a smart scan to refine a clients channel scans to just a few channels as opposed to all available channels. This option is disabled by default.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <p>wing-load-information</p>                                                               | <p>Enables support for the WiNG load information element (Element ID 173) with legacy Symbol Technology clients, thus making them optimally interoperable with the latest Extreme Networks access points. This option is enabled by default.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <p>wmm-load-information</p>                                                                | <p>Enables support for WiNG WMM (Wi-Fi MultiMedia) Load Information Element in radio transmissions with legacy clients. This option is disabled by default.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

### Examples

```

nx9500-6C8809(config-wlan-test)#wing-extensions wmm-load-information
nx9500-6C8809(config-wlan-test)#show context
wlan test
description TestWLAN
ssid test
bridging-mode local
encryption-type tkip-ccmp
authentication-type eap
kerberos server timeout 12
kerberos server primary host 172.16.10.2
accounting syslog host 172.16.10.4 port 2

```

```

data-rates 2.4GHz gn
wing-extensions wmm-load-information
client-load-balancing probe-req-intvl 5ghz 5
--More--
nx9500-6C8809(config-wlan-test)#

```

## Related Commands

|           |                                                                                                                                                          |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>no</b> | Disables support for WiNG-specific client extensions to the IEEE 802.11x WLAN standards. Use the keywords provided to disable a specific wing-extension. |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------|

## wireless-client

Configures the transmit power indicated to clients

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```

wireless-client [count-per-radio|cred-cache-ageout|hold-time|inactivity-timeout|
max-firewall-sessions|reauthentication|roam-notification|tx-power|t5-inactivity-timeout|
vlan-cache-out]
wireless-client [count-per-radio <0-256>|cred-cache-ageout <60-86400>|
hold-time <1-86400>|inactivity-timeout <60-86400>|max-firewall-sessions <10-10000>|
reauthentication <30-86400>|t5-inactivity-timeout <60-86400>|tx-power <0-20>|
vlan-cache-ageout <60-86400>]
wireless-client roam-notification [after-association|after-data-ready|auto]

```

### Parameters

```

wireless-client [count-per-radio <0-256>|cred-cache-ageout <60-86400>|
hold-time <1-86400>|inactivity-timeout <60-86400>|max-firewall-sessions <10-10000>|
reauthentication <30-86400>|t5-inactivity-timeout <60-86400>|tx-power <0-20>|
vlan-cache-ageout <60-86400>]

```

|                                  |                                                                                                                                                                                                                                                                             |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless-client                  | Configures the transmit power indicated to wireless clients for transmission                                                                                                                                                                                                |
| count-per-radio <0-256>          | Configures the maximum number of clients allowed on this WLAN per radio <ul style="list-style-type: none"> <li>• &lt;0-256&gt; – Specify a value from 0 - 256.</li> </ul>                                                                                                   |
| cred-cache-ageout <60-86400>     | Configures the timeout period for which client credentials are cached across associations <ul style="list-style-type: none"> <li>• &lt;60-86400&gt; – Specify a value from 60 - 86400 seconds.</li> </ul>                                                                   |
| hold-time <1-86400>              | Configures the time period for which wireless client state information is cached post roaming <ul style="list-style-type: none"> <li>• &lt;1-86400&gt; – Specify a value from 1 - 86400 seconds.</li> </ul>                                                                 |
| inactivity-timeout <60-86400>    | Configures an inactivity timeout period in seconds. If a frame is not received from a wireless client for this period of time, the client is disassociated. <ul style="list-style-type: none"> <li>• &lt;60-86400&gt; – Specify a value from 60 - 86400 seconds.</li> </ul> |
| max-firewall-sessions <10-10000> | Configures the maximum firewall sessions allowed per client on a WLAN <ul style="list-style-type: none"> <li>• &lt;10-10000&gt; – Specify the maximum number of firewall sessions allowed from 10 - 10000.</li> </ul>                                                       |

|                                     |                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| reauthentication<br><30-86400>      | Configures periodic reauthentication of associated clients <ul style="list-style-type: none"> <li>&lt;30-86400&gt; - Specify the client reauthentication interval from 30 - 86400 seconds.</li> </ul>                                                                                                                                              |
| t5-inactivity-timeout<br><60-86400> | Configures and inactivity timeout, in seconds, for T5 devices. When configured, the T5 device is disassociated if the time lapsed after the last frame received from it exceeds the value specified here. <ul style="list-style-type: none"> <li>&lt;60-86400&gt; - Specify a value from 60 - 86400 seconds. The default is 60 seconds.</li> </ul> |
| tx-power <0-20>                     | Configures the transmit power indicated to clients <ul style="list-style-type: none"> <li>&lt;0-20&gt; - Specify a value from 0 - 20 dBm.</li> </ul>                                                                                                                                                                                               |
| vlan-cache-ageout<br><60-86400>     | Configures the timeout period for which client VLAN information is cached across associations. <ul style="list-style-type: none"> <li>&lt;60-86400&gt; - Specify a value from 60 - 86400 seconds.</li> </ul>                                                                                                                                       |

wireless-client roam-notification [after-association|after-data-ready|auto]

|                   |                                                                                                                     |
|-------------------|---------------------------------------------------------------------------------------------------------------------|
| wireless-client   | Configures the transmit power indicated to wireless clients for transmission                                        |
| roam-notification | Configures when a roam notification is transmitted                                                                  |
| after-association | Transmits a roam notification after a client has associated                                                         |
| after-data-ready  | Transmits a roam notification after a client is data-ready (after completion of authentication, handshakes etc.)    |
| auto              | Transmits a roam notification upon client association (if the client is known to have authenticated to the network) |

### Examples

```

nx9500-6C8809(config-wlan-test)#wireless-client cred-cache-ageout 65
<exsw1>(config-wlan-test)#wireless-client hold-time 200
nx9500-6C8809(config-wlan-test)#wireless-client max-firewall-sessions 100
nx9500-6C8809(config-wlan-test)#wireless-client reauthentication 35
nx9500-6C8809(config-wlan-test)#wireless-client tx-power 12
nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid testWLAN1
 vlan-pool-member 1 limit 1
 vlan-pool-member 2 limit 1
 vlan-pool-member 3 limit 1
 vlan-pool-member 4 limit 1
 vlan-pool-member 5 limit 1
 vlan-pool-member 6 limit 1
 vlan-pool-member 7 limit 1
 vlan-pool-member 8 limit 1
 vlan-pool-member 9 limit 1
 vlan-pool-member 10 limit 1
 bridging-mode local
 encryption-type none
 authentication-type none
wireless-client hold-time 200
wireless-client cred-cache-ageout 65
wireless-client max-firewall-sessions 100
 protected-mgmt-frames mandatory
wireless-client reauthentication 35
 wep64 key 1 hex 0 7465737431
 wep128 key 1 hex 0 25f6e7ed9718918a87a75acc75
 wep128 key 2 hex 0 2b3fb36924b22dffe98c86c315

```

```
wep128 key 3 hex 0 1ebf3394431700194762ebd5b2
wep128 key 4 hex 0 e3de75be311bd787aeac5e4e8b
radius vlan-assignment
time-based-access days weekdays start 10:00 end 16:30
wing-extensions wmm-load-information
wireless-client tx-power 12
client-load-balancing probe-req-intvl 5ghz 5
--More--
nx9500-6C8809(config-wlan-test)#
```

#### Related Commands

|           |                                                                             |
|-----------|-----------------------------------------------------------------------------|
| <b>no</b> | Removes or reverts to default configured wireless client related parameters |
|-----------|-----------------------------------------------------------------------------|

### wpa-wpa2

Modifies TKIP-CCMP (WPA/WPA2) related parameters

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
wpa-wpa2 [exclude-wpa2-tkip|handshake|key-rotation|opp-pmk-caching|pmk-caching|
preauthentication|server-only-authentication|psk|tkip-countermeasures|use-sha256-akm]
wpa-wpa2 [exclude-wpa2-tkip|opp-pmk-caching|pmk-caching|preauthentication|
server-only-authentication|use-sha256-akm]
wpa-wpa2 handshake [attempts|init-wait|priority|timeout]
wpa-wpa2 handshake [attempts <1-5>|init-wait <5-1000000>|priority [high|normal]]
timeout <10-5000> {10-5000}]
wpa-wpa2 key-rotation [broadcast|unicast] <30-86400>
wpa-wpa2 psk [0 <LINE>|2 <LINE>|<LINE>]
wpa-wpa2 tkip-countermeasures holdtime <0-65535>
```

#### Parameters

```
wpa-wpa2 [exclude-wpa2-tkip|opp-pmk-caching|pmk-caching|preauthentication|
server-only-authentication|use-sha256-akm]
```

|                   |                                                                                                                                                |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| wpa-wpa2          | Modifies TKIP-CCMP (WPA/WPA2) related parameters                                                                                               |
| exclude-wpa2-tkip | Excludes the WPA2 (Wi-Fi Protected Access II) version of TKIP. It supports the WPA version of TKIP only. This option is disabled by default.   |
| opp-pmk-caching   | Uses opportunistic key caching (same PMK (Pairwise Master Key) across APs for fast roaming with EAP.802.1x. This option is enabled by default. |
| pmk-caching       | Uses cached pair-wise master keys (fast roaming with eap/802.1x). This option is enabled by default.                                           |
| preauthentication | Uses pre-authentication mode (WPA2 fast roaming)                                                                                               |
| use-sha256-akm    | Uses sha256 authentication key management suite                                                                                                |

```
wpa-wpa2 handshake [attempts <1-5>|init-wait <5-1000000>|priority [high|normal]]
timeout <10-5000> {10-5000}]
```

|           |                                                  |
|-----------|--------------------------------------------------|
| wpa-wpa2  | Modifies TKIP-CCMP (WPA/WPA2) related parameters |
| handshake | Configures WPA/WPA2 handshake parameters         |

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| attempts <1-5>                 | Configures the total number of times a message is transmitted towards a non-responsive client <ul style="list-style-type: none"> <li>• &lt;1-5&gt; – Specify a value from 1 - 5. The default is 2.</li> </ul>                                                                                                                                                                                                       |
| init-wait<br><5-1000000>       | Configures a minimum wait-time period, in microseconds, before the first handshake message is transmitted from the AP. This option is disabled by default. <ul style="list-style-type: none"> <li>• &lt;5-1000000&gt; – Specify a value from 5 - 1000000 microseconds.</li> </ul>                                                                                                                                   |
| priority [high normal]         | Configures the relative priority of handshake messages compared to other data traffic <ul style="list-style-type: none"> <li>• high – Treats handshake messages as high priority packets on a radio. This is the default setting.</li> <li>• normal – Treats handshake messages as normal priority packets on a radio</li> </ul>                                                                                    |
| timeout <10-5000><br><10-5000> | Configures the timeout period, in milliseconds, for a handshake message to retire. Once this period is exceeded, the handshake message is retired. <ul style="list-style-type: none"> <li>• &lt;10-5000&gt; – Specify a value from 10 - 5000 milliseconds. The default is 500 milliseconds.</li> <li>• &lt;10-5000&gt; – Optional. Configures a different timeout between the second and third attempts'</li> </ul> |

wpa-wpa2 key-rotation [broadcast|unicast] <30-86400>

|                         |                                                                                                                                                                                                                                                                                                                      |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wpa-wpa2                | Modifies TKIP-CCMP (WPA/WPA2) related parameters                                                                                                                                                                                                                                                                     |
| key-rotation            | Configures parameters related to periodic rotation of encryption keys. The periodic key rotation parameters are broadcast, multicast, and unicast traffic.                                                                                                                                                           |
| broadcast<br><30-86400> | Configures the periodic rotation of keys used for broadcast and multicast traffic. This parameter specifies the interval, in seconds, at which keys are rotated. This option is disabled by default. <ul style="list-style-type: none"> <li>• &lt;30-86400&gt; – Specify a value from 30 - 86400 seconds.</li> </ul> |
| unicast<br><30-86400>   | Configures a periodic interval for the rotation of keys, used for unicast traffic. This option is disabled by default. <ul style="list-style-type: none"> <li>• &lt;30-86400&gt; – Specify a value from 30 - 86400 seconds.</li> </ul>                                                                               |

wpa-wpa2 psk [0 <LINE>|2 <LINE>|<LINE>]

|          |                                                                                                                                   |
|----------|-----------------------------------------------------------------------------------------------------------------------------------|
| wpa-wpa2 | Modifies TKIP-CCMP (WPA/WPA2) related parameters                                                                                  |
| psk      | Configures a pre-shared key.                                                                                                      |
| 0 <LINE> | Configures a clear text key                                                                                                       |
| 2 <LINE> | Configures an encrypted key                                                                                                       |
| <LINE>   | Enter the pre-shared key either as a passphrase not exceeding 8 - 63 characters, or as a 64 character (256bit) hexadecimal value. |

wpa-wpa2 tkip-countermeasures holdtime <0-65535>

|                      |                                                                                                                                                                                                                                                                                          |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wpa-wpa2             | Modifies TKIP-CCMP (WPA/WPA2) parameters                                                                                                                                                                                                                                                 |
| tkip-countermeasures | Configures a hold time period for implementation of TKIP counter measures                                                                                                                                                                                                                |
| holdtime <0-65535>   | Configures the amount of time a WLAN is disabled when TKIP counter measures are invoked <ul style="list-style-type: none"> <li>&lt;0-65535&gt; - Specify a value from 0 - 65536 seconds. &lt;0-65535&gt; - Specify a value from 0 - 65535 seconds. The default is 60 seconds.</li> </ul> |

### Examples

```

nx9500-6C8809(config-wlan-test)#wpa-wpa2 tkip-countermeasures hold-time 2
nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid testWLAN1
 vlan-pool-member 1 limit 1
 vlan-pool-member 2 limit 1
 vlan-pool-member 3 limit 1
 vlan-pool-member 4 limit 1
 vlan-pool-member 5 limit 1
 vlan-pool-member 6 limit 1
 vlan-pool-member 7 limit 1
 vlan-pool-member 8 limit 1
 vlan-pool-member 9 limit 1
 vlan-pool-member 10 limit 1
 bridging-mode local
 encryption-type none
 authentication-type none
 wireless-client hold-time 200
 wireless-client cred-cache-ageout 65
 wireless-client max-firewall-sessions 100
 protected-mgmt-frames mandatory
 wireless-client reauthentication 35
 wpa-wpa2 tkip-countermeasures hold-time 2
 wep64 key 1 hex 0 7465737431
 wep128 key 1 hex 0 25f6e7ed9718918a87a75acc75
 --More--
nx9500-6C8809(config-wlan-test)#

```

### Related Commands

|    |                                                                       |
|----|-----------------------------------------------------------------------|
| no | Removes or reverts to default TKIP-CCMP (WPA/WPA2) related parameters |
|----|-----------------------------------------------------------------------|

### no (wlan-config-mode)

Negates WLAN mode commands and reverts values to their default

Supported in the following platforms:

- Access Points — AP 6522, AP 6532, AP 6562, AP 7502, AP 7522, AP 7532, AP 7161, AP 81XX, AP 8232
- Wireless Controllers — RFS 4000, RFS 6000
- Service Platforms — NX 7500, NX 9500, NX 9510

### Syntax

```
no <PARAMETERS>
```

### Parameters

None

### Usage Guidelines

The *no* command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

### Examples

|                                                    |                                                                                        |
|----------------------------------------------------|----------------------------------------------------------------------------------------|
| <code>nx9500-6C8809(config-wlan-test)#no ?</code>  |                                                                                        |
| <code>accounting</code>                            | Configure how accounting records are created for this wlan                             |
| <code>acl</code>                                   | Actions taken based on ACL configuration [ packet drop being one of them]              |
| <code>answer-broadcast-probes</code>               | Do not Include this wlan when responding to probe requests that do not specify an SSID |
| <code>assoc-response</code>                        | Association response threshold                                                         |
| <code>association-list</code>                      | Configure the association list for the wlan                                            |
| <code>authentication-type</code>                   | Reset the authentication to use on this wlan to default (none/Pre-shared keys)         |
| <code>broadcast-dhcp</code>                        | Configure broadcast DHCP packet handling                                               |
| <code>broadcast-ssid</code>                        | Do not advertise the SSID of the WLAN in beacons                                       |
| <code>captive-portal-enforcement</code>            | Configure how captive-portal is enforced on the wlan                                   |
| <code>client-access</code>                         | Disallow client access on this wlan (no data operations)                               |
| <code>client-client-communication</code>           | Disallow switching of frames from one wireless client to another on this wlan          |
| <code>client-load-balancing</code>                 | Disable load-balancing of clients on this wlan                                         |
| <code>controller-assisted-mobility</code>          | Disable configure assisted mobility                                                    |
| <code>data-rates</code>                            | Reset data rate configuration to default                                               |
| <code>description</code>                           | Reset the description of the wlan                                                      |
| <code>downstream-group-addressed-forwarding</code> | Disable downstream group addressed forwarding of packets                               |
| <code>dpi</code>                                   | Deep-Packet-Inspection (Application Assurance)                                         |
| <code>dynamic-vlan-assignment</code>               | Dynamic VLAN assignment configuration                                                  |
| <code>eap-types</code>                             | Allow all EAP types on this wlan                                                       |
| <code>encryption-type</code>                       | Reset the encryption to use on this wlan to default (none)                             |
| <code>enforce-dhcp</code>                          | Drop packets from Wireless Clients with static IP address                              |
| <code>fast-bss-transition</code>                   | Disable support for 802.11r Fast BSS Transition                                        |
| <code>http-analyze</code>                          | Enable HTTP URL analysis on the wlan                                                   |
| <code>ip</code>                                    | Internet Protocol (IP)                                                                 |
| <code>ipv6</code>                                  | Internet Protocol version 6 (IPv6)                                                     |
| <code>kerberos</code>                              | Configure kerberos authentication parameters                                           |
| <code>mac-authentication</code>                    | Configure mac-authentication related parameters                                        |
| <code>nsight</code>                                | Nsight Server                                                                          |
| <code>opendns</code>                               | OpenDNS related config for this wlan                                                   |
| <code>protected-mgmt-frames</code>                 | Disable support for Protected Management Frames (IEEE 802.11w)                         |
| <code>proxy-arp-mode</code>                        | Configure handling of ARP requests with proxy-arp is enabled                           |
| <code>proxy-nd-mode</code>                         | Configure handling of IPv6 ND requests with proxy-nd is enabled                        |
| <code>qos-map</code>                               | Disable the 802.11u QoS map element                                                    |



|                            |                                                                     |
|----------------------------|---------------------------------------------------------------------|
| radio-resource-measurement | and frame<br>Disable support for 802.11k Radio Resource Measurement |
| radius                     | Configure RADIUS related parameters                                 |
| registration               | Dynamic registration of device (or) user                            |
| relay-agent                | Configure dhcp relay agent info                                     |
| shutdown                   | Enable the use of this wlan                                         |
| ssid                       | Configure ssid                                                      |
| t5-client-isolation        | Do not Isolate traffic among clients                                |
| t5-security                | Configure encryption and authentication                             |
| time-based-access          | Reset time-based-access parameters to default                       |
| use                        | Set setting to use                                                  |
| vlan                       | Map the default vlan (vlan-id 1) to the wlan                        |
| vlan-pool-member           | Delete a mapped vlan from this wlan                                 |
| wep128                     | Reset WEP128 parameters                                             |
| wep64                      | Reset WEP64 parameters                                              |
| wing-extensions            | Disable support for WiNG-Specific extensions to 802.11              |
| wireless-client            | Configure wireless-client specific parameters                       |
| wpa-wpa2                   | Modify tkip-ccmp (wpa/wpa2) related parameters                      |
| service                    | Service to monitor to show no-service page to user                  |

```
nx9500-6C8809(config-wlan-test)#
```

The WLAN 'test' settings before execution of the no command:

```
nx9500-6C8809(config-wlan-test)#show context
wlan test
 description TestWLAN
 ssid test
 bridging-mode local
 encryption-type tkip-ccmp
 authentication-type eap
 kerberos server timeout 12
 kerberos server primary host 172.16.10.2
 accounting syslog host 172.16.10.4 port 2
 data-rates 2.4GHz gn
 wing-extensions wmm-load-information
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 captive-portal-enforcement fall-back
 ip dhcp trust
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 enforce-dhcp
 broadcast-dhcp validate-offer
 http-analyze controller
nx9500-6C8809(config-wlan-test)#
nx9500-6C8809(config-wlan-test)#no accounting syslog
nx9500-6C8809(config-wlan-test)#no description
nx9500-6C8809(config-wlan-test)#no authentication-type
nx9500-6C8809(config-wlan-test)#no encryption-type
nx9500-6C8809(config-wlan-test)#no enforce-dhcp
nx9500-6C8809(config-wlan-test)#no kerberos server primary host
nx9500-6C8809(config-wlan-test)#no kerberos server timeout
nx9500-6C8809(config-wlan-test)#no data-rates 2.4GHz
nx9500-6C8809(config-wlan-test)#no ip dhcp trust
nx9500-6C8809(config-wlan-test)#no captive-portal-enforcement
```

The WLAN 'test' settings after the execution of the no command:

```
nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode local
 encryption-type none
 authentication-type none
 wing-extensions wmm-load-information
 client-load-balancing probe-req-intvl 5ghz 5
 client-load-balancing band-discovery-intvl 2
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
 broadcast-dhcp validate-offer
 http-analyze controller
nx9500-6C8809(config-wlan-test)#
```

### *wlan-qos-policy*

Configures a WLAN QoS policy and enters its configuration mode

#### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### **Syntax**

```
wlan-qos-policy <WLAN-QOS-POLICY-NAME>
```

#### **Parameters**

```
wlan-qos-policy <WLAN-QOS-POLICY-NAME>
```

|                        |                                                                                                      |
|------------------------|------------------------------------------------------------------------------------------------------|
| <WLAN-QOS-POLICY-NAME> | Specify the WLAN QoS policy name. If a policy with the specified name does not exist, it is created. |
|------------------------|------------------------------------------------------------------------------------------------------|

#### **Examples**

```
nx9500-6C8809(config)#wlan-qos-policy test
nx9500-6C8809(config-wlan-qos-test)#?
WLAN QoS Mode commands:
 accelerated-multicast Configure accelerated multicast streams address and
 forwarding QoS classification
 classification Select how traffic on this WLAN must be classified
 (relative prioritization on the radio)
 multicast-mask Egress multicast mask (frames that match bypass the
 PSPqueue. This permits intercom mode operation
 without delay even in the presence of PSP clients)
 no Negate a command or set its defaults
 qos Quality of service
 rate-limit Configure traffic rate-limiting parameters on a
 per-wlan/per-client basis
 svp-prioritization Enable spectralink voice protocol support on this
 wlan
 voice-prioritization Prioritize voice client over other client (for
 non-WMM clients)
 wmm Configure 802.11e/Wireless MultiMedia parameters

 clrscr Clears the display screen
 commit Commit all changes made in this session
```

```

do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

```

```
nx9500-6C8809(config-wlan-qos-test)#
```

## Related Commands

|           |                              |
|-----------|------------------------------|
| <b>no</b> | Removes an existing WLAN QoS |
|-----------|------------------------------|



### Note

For more information on WLAN QoS policy commands, see [WLAN-QoS-POLICY](#).

## *url-filter*

Creates a new URL filter (Web filter) and enters its configuration mode. URL filtering is a licensed feature. When applied to a WiNG device the license allows you to enable URL filtering on the device, create and apply a URL filter defining the banned and/or allowed URLs. When enabled, the URL filter is applied to all user-initiated URL requests to determine if the requested URL is banned or allowed. Only if allowed is the user's request (in the form of a HTTP request packet) forwarded to the Web server.

URL filters can be applied at any of the following points: the user's application (browser/email reader), the network's gateway, at the ISP's (Internet service provider) end, and also on a Web portal. For wireless clients, the WLAN infrastructure is the best place to implement these filters.

A URL filter is a set of whitelist and/or blacklist rules. The whitelist allows access only to those Websites and URLs specified in it. All other Websites and URLs, apart from those specified in the whitelist, are banned. On the other hand, the blacklist bans all Websites and URLs specified in it. All other Websites and URLs, apart from those specified in the blacklist, are allowed.

To simplify URL filter configuration, Websites have been classified into pre-defined category-types and categories. The system provides 12 category-types and 64 categories. To further simplify configuration, these 12 category-types have been grouped into five (5) pre-defined levels. (See Usage Guidelines section for the list of category-types, categories, and levels). The actual classification of URLs (on the basis of the pre-defined factors mentioned above) is done by the classification server. A local database also helps by caching URL records for a user-defined time period. The classification server host is specified in the Web filter policy. The Web filter policy also defines the URL database parameters. For more information, see [web-filter-policy](#).

The WiNG software also allows you to create URL lists. Each URL list contains a list of user-defined URLs. Use the URL list in a URL filter (whitelist or blacklist rule) to identify the URLs to ban or allow. For example, a URL list named SocialNetworking is created listing the following three sites: Facebook, Twitter, and LinkedIn. When applied to a URL filter's blacklist these three sites are banned. Where as,

when applied to a whitelist only these three sites are allowed. For more information on configuring a URL list, see [url-list](#).



**Note**

URL filtering is a licensed feature. Procure and install the license in the device configuration mode. For more information, see [license](#) on page 1267 (device config mode).

**Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

**Syntax**

`url-filter <URL-FILTER-NAME>`

**Parameters**

`url-filter <URL-FILTER-NAME>`

|                                      |                                                                                                                                                             |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;URL-FILTER-NAME&gt;</code> | Creates a new URL filter and enters its configuration mode. Specify the URL filter name. If a filter with the specified name does not exist, it is created. |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Usage Guidelines**

| SI No. | Category Type           | Category                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1      | Adult Content           | Alcohol & Tobacco, Dating & Personals, Gambling, Nudity, Pornography/Sexually Explicit, Sex Education, Weapons                                                                                                                                                                                                                                                                                                                                        |
| 2      | Business                | Web-based Email                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 3      | Communication           | Chat, Instant Messaging                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 4      | Entertainment           | Streaming Media & Downloads                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 5      | File Sharing and Backup | Download Sites                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 6      | Gaming                  | Games                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 7      | News Sports and General | Arts, Business, Computer & Technology, Education, Entertainment, Fashion & Beauty, Finance, Forum & Newsgroups, General, Government, Greeting Card, Health & Medicine, Information Security, Job Search, Leisure & Recreation, Network Errors, News, Non-Profits & NGO, Personal Sites, Politics, Private IP Addresses, Real Estates, Religion, Restaurants & Dinning, Search Engine & Portals, Shopping, Sports, Transportation, Translators, Travel |
| 8      | Peer-to-Peer (P2P)      | Peer to Peer                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 9      | Questionable/Unethical  | Child Abuse Images, Cults, Hacking, Hate & Intolerance, Illegal Drug, Illegal Sharing, Illegal Software, School Cheating, Tasteless, Violence                                                                                                                                                                                                                                                                                                         |
| 10     | Security Risk           | Advertisement & Pop-ups, Anonymizers, Botnets, Compromised, Criminal Activity, Malware, Parked Domains, Phishing & Fraud, Spam Sites                                                                                                                                                                                                                                                                                                                  |

| SI No. | Category Type            | Category          |
|--------|--------------------------|-------------------|
| 11     | Social and Photo Sharing | Social Networking |
| 12     | Software Update          | N/A               |

| SI No. | Level       | Description                                                                                          |
|--------|-------------|------------------------------------------------------------------------------------------------------|
| 1      | Basic       | Blocks sites/URL categorized as Security Risk                                                        |
| 2      | Low         | Blocks sites/URL categorized as Adult Content + Basic                                                |
| 3      | Medium      | Blocks sites/URL categorized as File Sharing and Backup, P2P, Questionable / Unethical + Low         |
| 4      | Medium High | Blocks sites/URL categorized as Gaming + Medium                                                      |
| 5      | High        | Blocks sites/URL categorized as Communication, Entertainment, Social and Photo Sharing + Medium High |

### Examples

```

nx9500-6C8809(config-url-filter-test)#?
URL Filter Mode commands:
 blacklist Block access to URL
 blockpage Configure blocking page parameters
 description Url filter description
 no Negate a command or set its defaults
 whitelist Allow access to URL

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

```

```
nx9500-6C8809(config-url-filter-test)#
```

### Related Commands

|                 |                                       |
|-----------------|---------------------------------------|
| <code>no</code> | Removes an existing URL filter policy |
|-----------------|---------------------------------------|

### url-filter-config-commands

The following table summarizes URL filter configuration mode commands:

**Table 31: URL Filter Config Mode Commands**

| Command                            | Description                                                                                                                                        |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>blacklist</code> on page 626 | Creates a blacklist rule defining a list of banned Websites and URLs                                                                               |
| <code>blockpage</code> on page 628 | Configures the parameters that retrieve the page or content displayed by the client's browser when a requested URL is blocked and cannot be viewed |

**Table 31: URL Filter Config Mode Commands (continued)**

| Command                                 | Description                                                                              |
|-----------------------------------------|------------------------------------------------------------------------------------------|
| <a href="#">description</a> on page 629 | Configures an appropriate description for this URL filter                                |
| <a href="#">whitelist</a> on page 630   | Creates a whitelist rule defining a list of Websites and URLs allowed access by clients. |
| <a href="#">no</a> on page 632          | Removes this URL filter's configured parameters                                          |

## blacklist

Creates a blacklist rule. A blacklist is a list of Websites and URLs denied access by clients. Clients requesting blacklisted URLs are presented with a page displaying the 'Web page blocked' message. Parameters relating to this page are configured using the 'blockpage' option.

URL filtering is based on the classification of Websites into pre-defined category-types. Some of the category-types are further divided into multiple categories. Currently available are 12 built-in category types, and 64 categories. These built-in category-types and categories cannot be modified.

Use the available options to identify the URL category-types and categories to include in the blacklist.

In addition to identifying URLs by the categories and category-types they are classified into, the system also provides five (5) levels of Web filtering (basic, high, low, medium, and medium-high). Each level identifies a specific set of URL categories to blacklist. For more information on category-types, categories, and URL filtering levels, see [url-filter](#).

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
blacklist [category-type|level|url-list]
blacklist category-type [adult-content|all|business|communication|entertainment|
file-sharing-backup|gaming|news-sports-general|p2p|questionable|security-risk|
social-photo-sharing|software-updates] precedence <1-500> {description <LINE>}
blacklist level [basic|high|low|medium|medium-high] precedence <1-500>
{description <LINE>}
blacklist url-list <URL-LIST-NAME> precedence <1-500> {description <LINE>}
```

### Parameters

```
blacklist category-type [adult-content|all|business|communication|entertainment|
file-sharing-backup|gaming|news-sports-general|p2p|questionable|security-risk|social-photo-
sharing|
software-updates] precedence <1-500> {description <LINE>}
```

|                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| blacklist category-type<br><SELECT-CATEGORY-TYPE> | <p>Selects the category-type to blacklist. A category is a pre-defined URL list available in the WiNG software. Categories are based on an external database, and cannot be modified or removed. Custom categories can be created with the URL List and added to the database.</p> <p>Websites have been classified into the following 12 category types: adult-content, business, communication, entertainment, file-sharing-backup, gaming, news-sports-general, p2p, questionable, security-risk, social-photo-sharing, and software-updates</p> <p>Select 'all' to blacklist all category-types.</p> <p>Some of the category-types are further classified into categories. For example, the 'adult-content' category-type is differentiated into the following categories:</p> <ul style="list-style-type: none"> <li>• alcohol-tobacco, dating-personals, gambling, nudity, pornography-sexually-explicit, sex-education, and weapons.</li> </ul> <p>The system blocks all categories (URLs falling within their limits) within the selected category-type.</p> |
| precedence <1-500>                                | Configures the precedence value for this blacklist rule. Rules are applied in the increasing order of their precedence. Therefore, rules with lower precedence are applied first.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| description <LINE>                                | Optional. Configures a description (not exceeding 80 characters) for this blacklist rule. Enter a description that allows you to identify the purpose of the rule.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

```
blacklist level [basic|high|low|medium|medium-high] precedence <1-500> {description <LINE>}
```

|                                                     |                                                                                                                                                                                                    |
|-----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| blacklist level [basic high low medium medium-high] | Configures the Web filtering level as basic, high, low, medium, or medium-high. Each of these filter-levels are pre-configured to use a set of category types and this mapping cannot be modified. |
| precedence <1-500>                                  | Configures the precedence value for this blacklist rule. Rules are applied in the increasing order of their precedence. Therefore, rules with lower precedence are applied first.                  |
| description <LINE>                                  | Optional. Configures a description (not exceeding 80 characters) for this blacklist rule. Enter a description that allows you to identify the purpose of the rule.                                 |

```
blacklist url-list <URL-LIST-NAME> precedence <1-500> {description <LINE>}
```

|                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| blacklist url-list <URL-LIST-NAME> | <p>Associates a URL list with this URL filter. When associated with a blacklist rule, all URLs listed in the specified URL list are blacklisted.</p> <p>URL lists are customized categories included in the custom filter-level setting. URL lists enable an administrator to blacklist or whitelist URLs in addition to the built-in categories. For more information on configuring a URL list, see <a href="#">url-list</a>.</p> <ul style="list-style-type: none"> <li>• &lt;URL-LIST-NAME&gt; – Enter URL list name (should be existing and configured)</li> </ul> |
| precedence <1-500>                 | Configures the precedence value for this blacklist rule. Rules are applied in the increasing order of their precedence. Therefore, rules with lower precedence are applied first.                                                                                                                                                                                                                                                                                                                                                                                       |
| description <LINE>                 | Optional. Configures a description (not exceeding 80 characters) for this blacklist rule. Enter a description that allows you to identify the purpose of the rule.                                                                                                                                                                                                                                                                                                                                                                                                      |

## Examples

```
nx9500-6C8809(config-url-filter-test)#blacklist level medium-high precedence 10
nx9500-6C8809(config-url-filter-test)#blacklist category-type adult-content category
alcohol-tobacco precedence 1
nx9500-6C8809(config-url-filter-test)#blacklist category-type security-risk category
botnets precedence 3
nx9500-6C8809(config-url-filter-test)#show context
url-filter test
 blacklist level medium-high precedence 10
 blacklist category-type security-risk category botnets precedence 3
 blacklist category-type adult-content category alcohol-tobacco precedence 1
nx9500-6C8809(config-url-filter-test)#
```

## Related Commands

|                             |                                                                                                                                                                                        |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>no</code> on page 632 | Removes a blacklist rule from this URL filter. Specify the category-type, category, and precedence to identify the blacklist rule. The identified rule is removed from the URL filter. |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## blockpage

Configures the parameters that retrieve the page or content displayed by the client's browser when a requested URL is blocked and cannot be viewed

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
blockpage [external|internal|path]
blockpage path [external|internal]
blockpage external url <URL>
blockpage internal [content|footer|header|main-logo|org-name|org-signature|
small-logo|title] <LINE/IMAGE-URL>
```

## Parameters

```
blockpage path [external|internal]
```

|                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>blockpage path [external internal]</code> | Specifies if the location of the page displayed, to the client when a requested URL is blocked, is external or internal <ul style="list-style-type: none"><li>• external – Indicates the page displayed is hosted on an external Web server resource. If selecting this option, use the <b>blockpage &gt; external &gt; url &lt;URL&gt;</b> command to provide the path to the external Web server hosting the page.</li><li>• internal – Indicates the page displayed is hosted internally. This is the default setting. If selecting this option, use the <b>blockpage &gt; internal &gt; &lt;SELECT-PAGE-TYPE&gt; &gt; &lt;LINE/IMAGE-URL&gt;</b> command to define the page configuration.</li></ul> |
|-------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
blockpage external url <URL>
```



|                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>blockpage external url &lt;URL&gt;</pre> | <p>Configures the URL of the external Web server hosting the page (displayed to the client when a requested URL is blocked).</p> <ul style="list-style-type: none"> <li>url &lt;URL&gt; - Specify the URL of the Web server and the blocking page name</li> </ul> <p>Valid URLs should begin with http:// or https://<br/>The URL can contain query strings.<br/>Use '&amp;' or '?' character to separate field-value pair.<br/>Enter 'ctrl-v' followed by '?' to configure query strings</p> |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
blockpage internal [content|footer|header|main-logo|org-name|org-signature|
small-logo|title] <LINE/IMAGE-URL>
```

|                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>blockpage internal [content  footer header main-logo org- name org-signature  small-logo  title] &lt;LINE/IMAGE-URL&gt;</pre> | <p>Configures the internally hosted blocking page parameters, such as the content displayed, page footer and header, organization (the organization enforcing the Web page blocking) details (name, signature, and logo), and page title</p> <ul style="list-style-type: none"> <li>content - Configures the text (message) displayed on the blocking page</li> <li>footer - Configures the text displayed as the blocking page footer</li> <li>header - Configures the text displayed as the blocking page header</li> <li>org-name - Configures the organization's name displayed on the blocking page</li> <li>org-signature - Configures the organization's signature displayed on the blocking page</li> <li>title - Configures the title of the blocking page.</li> <li>main-logo - Configures the location of the main logo (organization's large logo)</li> <li>small-logo - Configures the location of the small logo (organization's small logo)</li> </ul> <p>The following keyword is common to all of the above parameters:</p> <ul style="list-style-type: none"> <li>&lt;LINE/IMAGE-URL&gt; - Specify the location of the logo (main and small) image file. The image is retrieved and displayed from the location configured here. If you are using this option to provide content, such as organization name, footer, header, etc. enter a text string not exceeding 255 characters in length.</li> </ul> |
|------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config-url-filter-test)#blockpage internal content "The requested Web page
is blocked and cannot be displayed for viewing"
nx9500-6C8809(config-url-filter-test)#show context
url-filter test
 blacklist level medium-high precedence 10
 blacklist category-type security-risk category botnets precedence 3
 blacklist category-type adult-content category alcohol-tobacco precedence 1
blockpage internal content "The requested Web page is blocked and cannot be displayed for
viewing"
nx9500-6C8809(config-url-filter-test)#
```

### Related Commands

|                           |                                                 |
|---------------------------|-------------------------------------------------|
| <pre>no on page 632</pre> | <p>Removes the blocking page configurations</p> |
|---------------------------|-------------------------------------------------|

description

Configures a description for this URL filter. Provide a description that enables you to identify the purpose of this URL filter.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
description <LINE>
```

#### Parameters

```
description <LINE>
```

|                    |                                                                                                                                                               |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| description <LINE> | Enter an appropriate description for this URL filter. The description should identify the URL filter's purpose and should not exceed 80 characters in length. |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config-url-filter-test)#description "Blacklists sites inappropriate for children and are security risks."
nx9500-6C8809(config-url-filter-test)#show context
url-filter test
 description "Blacklists sites inappropriate for children and are security risks."
 blacklist level medium-high precedence 10
 blacklist category-type security-risk category botnets precedence 3
 blacklist category-type adult-content category alcohol-tobacco precedence 1
 blockpage internal content "The requested Web page is blocked and cannot be displayed for viewing"
nx9500-6C8809(config-url-filter-test)#
```

#### Related Commands

|                |                                       |
|----------------|---------------------------------------|
| no on page 632 | Removes this URL filter's description |
|----------------|---------------------------------------|

## whitelist

Creates a whitelist rule. A whitelist is a list of Websites and URLs allowed access by clients.

URL filtering is based on the classification of Websites into pre-defined category-types. Some of the category-types are further divided into multiple categories. Currently available are 12 built-in category types, and 64 categories. These built-in category-types and categories cannot be modified.

Use the available options to identify the category-types and categories to include in the whitelist.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
whitelist [category-type|url-list]
whitelist category-type [adult-content|all|business|communication|entertainment|
file-sharing-backup|gaming|news-sports-general|p2p|questionable|security-risk|
social-photo-sharing|software-updates] precedence <1-500> {description <LINE>}
```

## Parameters

```
whitelist category-type [adult-content|all|business|communication|entertainment|
file-sharing-backup|gaming|news-sports-general|p2p|questionable|security-risk|
social-photo-sharing|software-updates] precedence <1-500> {description <LINE>}
```

|                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| whitelist category-type <SELECT-CATEGORY-TYPE> | <p>Selects the category-type to add to this whitelist. A category is a pre-defined URL list available in the WiNG software. Categories are based on an external database, and cannot be modified or removed. Custom categories can be created with the URL List and added to the database.</p> <p>Websites have been classified into the following 12 category types: adult-content, business, communication, entertainment, file-sharing-backup, gaming, news-sports-general, p2p, questionable, security-risk, social-photo-sharing, and software-updates.</p> <p>Select 'all' to whitelist all category-types.</p> <p>Some of the category-types are further classified into categories. For example, the 'adult-content' category-type is differentiated into the following categories:</p> <ul style="list-style-type: none"> <li>• alcohol-tobacco, dating-personals, gambling, nudity, pornography-sexually-explicit, sex-education, and weapons.</li> </ul> <p>The system allows all categories (URLs falling within their limits) within the selected category-type.</p> |
| precedence <1-500>                             | Configures the precedence value for this whitelist rule. Rules are applied in the increasing order of their precedence. Therefore, rules with lower precedence are applied first.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| description <LINE>                             | Optional. Configures a description (not exceeding 80 characters) for this whitelist rule. Enter a description that allows you to identify the purpose of the rule.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

```
whitelist url-list <URL-LIST-NAME> precedence <1-500> {description <LINE>}
```

|                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| whitelist url-list <URL-LIST-NAME> | <p>Associates a URL list with this URL filter. When associated with a whitelist rule, all URLs listed in the specified URL list are allowed access.</p> <p>URL lists are customized categories included in the custom filter-level setting. URL lists enable an administrator to blacklist or whitelist URLs in addition to the built-in categories. For more information on configuring a URL list, see <a href="#">url-list</a>.</p> <ul style="list-style-type: none"> <li>• &lt;URL-LIST-NAME&gt; - Enter URL list name (should be existing and configured)</li> </ul> |
| precedence <1-500>                 | Configures the precedence value for this whitelist rule. Rules are applied in the increasing order of their precedence. Therefore, rules with lower precedence are applied first.                                                                                                                                                                                                                                                                                                                                                                                          |
| description <LINE>                 | Optional. Configures a description (not exceeding 80 characters) for this whitelist rule. Enter a description that allows you to identify the purpose of the rule.                                                                                                                                                                                                                                                                                                                                                                                                         |

## Examples

```
nx9500-6C8809(config-url-filter-test)#whitelist category-type communication category chat
precedence 7
nx9500-6C8809(config-url-filter-test)#show context
url-filter test
description "Blacklists sites inappropriate for children and are security risks."
blacklist level medium-high precedence 10
whitelist category-type communication category chat precedence 7
blacklist category-type security-risk category botnets precedence 3
blacklist category-type adult-content category alcohol-tobacco precedence 1
```

```
blockpage internal content "The requested Web page is blocked and cannot be displayed for viewing"
nx9500-6C8809(config-url-filter-test)#
```

## Related Commands

|                |                                                                                                                                                                                        |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| no on page 632 | Removes a whitelist rule from this URL filter. Specify the category-type, category, and precedence to identify the blacklist rule. The identified rule is removed from the URL filter. |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

no

Use the no command to remove this URL filter's configured parameters

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
no [blacklist|blockpage|description|whitelist]
no blacklist [category-type|level|url-list]
no blacklist [category-type <SELECT-CATEGORY-TYPE>|level <SELECT-LEVEL>|
url-list <URL-LIST-NAME>] precedence <1-500>
no blockpage [external|internal [content|footer|header|main-logo|org-name|
org-signature|small-logo|title]|path]
no description
no whitelist [category-type|url-list]
no whitelist [category-type <SELECT-CATEGORY-TYPE>|url-list <URL-LIST-NAME>]
precedence <1-500>
```

## Parameters

```
no <PARAMETERS>
```

|                 |                                                                                 |
|-----------------|---------------------------------------------------------------------------------|
| no <PARAMETERS> | Removes this URL filter's configured parameters based on the values passed here |
|-----------------|---------------------------------------------------------------------------------|

## Examples

The following example displays the URL filter 'test' settings before the 'no' is executed:

```
nx9500-6C8809(config-url-filter-test)#show context
url-filter test
 description "Blacklists sites inappropriate for children and are security risks."
 blacklist level medium-high precedence 10
 whitelist category-type communication category chat precedence 7
 blacklist category-type security-risk category botnets precedence 3
 blacklist category-type adult-content category alcohol-tobacco precedence 1
 blockpage internal content "The requested Web page is blocked and cannot be displayed for viewing"
nx9500-6C8809(config-url-filter-test)#
nx9500-6C8809(config-url-filter-test)#no description
nx9500-6C8809(config-url-filter-test)#no blacklist category-type adult-content
category alcohol-tobacco precedence 1
nx9500-6C8809(config-url-filter-test)#no whitelist category-type communication
category chat precedence 7
```

The following example displays the URL filter 'test' settings after the 'no' is executed:

```
nx9500-6C8809(config-url-filter-test)#show context
url-filter test
 blacklist level medium-high precedence 10
 blacklist category-type security-risk category botnets precedence 3
 blockpage internal content "The requested Web page is blocked and cannot be displayed for
viewing"
nx9500-6C8809(config-url-filter-test)#
```

### *url-list*

Creates a URL list and enters its configuration mode. URL lists are a means of categorizing URLs on the basis of various criteria, such as frequently used, not-permitted, etc. It is used in URL filters to identify whitelisted/blacklisted URLs. Web requests are blocked or approved based on URL filter whitelist/blacklist rules. A whitelist bans all sites except the categories and URL lists defined in the whitelist. The blacklist allows all sites except the categories and URL lists defined in the blacklist.

#### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### **Syntax**

```
url-list <URL-LIST-NAME>
```

#### **Parameters**

```
url-list <URL-LIST-NAME>
```

<URL-LIST-NAME> • Specify the URL list name. The URL list is created if another list with the same name does not exist.

#### **Examples**

```
nx9500-6C8809(config)#url-list URLlist1
nx9500-6C8809(config-url-list-URLlist1)#?
URL List Mode commands:
 description Description of the category
 no Negate a command or set its defaults
 url Add a URL entry

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-url-list-URLlist1)#
nx9500-6C8809(config-url-list-URLlist1)#url http://www.example_company.com depth 10
nx9500-6C8809(config-url-list-test)#show context
url-list test
```

```
url http://www.example_company.com depth 10
nx9500-6C8809(config-url-list-URLlist1)#
```

### Related Commands

|    |                              |
|----|------------------------------|
| no | Removes an existing URL list |
|----|------------------------------|

### url-list-config-commands

The following table summarizes URL list configuration mode commands:

**Table 32: URL List Config Mode Commands**

| Command                 | Description                                                           |
|-------------------------|-----------------------------------------------------------------------|
| url on page 634         | Adds URL entries to this URL list                                     |
| description on page 634 | Creates a blacklist rule defining a list of banned Web sites and URLs |
| no on page 635          | Removes this URL list's settings                                      |

### description

Configures a description for this URL list. The description should be unique and enable you to identify the type of URLs listed in the URL list.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
description <LINE>
```

### Parameters

```
description <LINE>
```

|                    |                                                                                              |
|--------------------|----------------------------------------------------------------------------------------------|
| description <LINE> | Provide a unique description for this URL list (should not exceed 500 characters in length). |
|--------------------|----------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config-url-list-test)#description ""This URL list contains social media
URLs.""
nx9500-6C8809(config-url-list-test)#show context
url-list test
 description "This URL list contains social media URLs."
nx9500-6C8809(config-url-list-test)#
```

### Related Commands

|                |                                     |
|----------------|-------------------------------------|
| no on page 635 | Removes this URL list's description |
|----------------|-------------------------------------|

### url

Adds URL entries to this URL list

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
url <WORD> {depth <1-10>}
```

Parameters

```
url <WORD> {depth <1-10>}
```

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| url <WORD> {depth <1-10>} | Adds a URL entry <ul style="list-style-type: none"><li>• &lt;WORD&gt; - Specify the URL to add.</li><li>• depth - Optional. Sets number of levels to be cached. Since Web sites have different parameters to uniquely identify specific content, the same content may be stored on multiple origin servers. Smart caching uses subsets of these parameters to recognize that the content is the same and serves it from cache.<ul style="list-style-type: none"><li>&lt;1-10&gt; - Specify the depth from 1 - 10.</li></ul></li></ul> |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Examples

```
nx9500-6C8809(config-url-list-test)#url http://www.facebook.com depth 5
nx9500-6C8809(config-url-list-test)#show context
url-list test
 description "This URL list contains social media URLs."
 url https://www.facebook.com depth 5
nx9500-6C8809(config-url-list-test)#
```

Related Commands

|                |                                        |
|----------------|----------------------------------------|
| no on page 635 | Removes a URL entry from this URL list |
|----------------|----------------------------------------|

no

Removes this URL list's settings

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
no [description|url]
no description
no url <WORD>
```

Parameters

```
no <PARAMETERS>
```

|                 |                                                            |
|-----------------|------------------------------------------------------------|
| no <PARAMETERS> | Removes this URL's settings based on the parameters passed |
|-----------------|------------------------------------------------------------|

Examples

The following example displays the URL list 'test' settings before the 'no' command is executed:

```
nx9500-6C8809(config-url-list-test)#show context
url-list test
 description "This URL list contains social media URLs."
 url https://www.facebook.com depth 5
nx9500-6C8809(config-url-list-test)#
nx9500-6C8809(config-url-list-test)#no url www.facebook.com
```

The following example displays the URL list 'test' settings after the 'no' command is executed:

```
nx9500-6C8809(config-url-list-test)#show context
url-list test
 description "This URL list contains social communication URLs"
nx9500-6C8809(config-url-list-test)#
```

## vx9000

Configures a Virtual WLAN Controller (V-WLC) in a VM (virtual machine) environment. V-WLC can be deployed on a shared, third-party server hardware, thereby reducing overhead costs of procuring and maintaining dedicated appliances. The external, third-party hardware needs to have installed hypervisors, such as VmWare, Xen, VirtualBox, KVM, Amazon EC2 or Hyper-V, enabling it to communicate with V-WLC software.

The V-WLC controls and manages access points and other controllers (at NOC or as a site-controller) in the network. The traffic between the access points and the V-WLC is over the layer-3 MINT protocol.

V-WLC is a licensed feature, and the WiNG software provides the following two new licenses:

- VX – When installed, this license activates VM controller instance, and enables the V-WLC to trigger adoption process allowing access points to adopt to the V-WLC. The adoption capacity of the V-WLC is determined by the number of licenses installed on it.
- VX – When installed, this license activates VM controller instance, and enables the V-WLC to trigger adoption process allowing access points to adopt to the V-WLC. The adoption capacity of the V-WLC is determined by the number of licenses installed on it.

To install the VX or VX-DEMO license on an existing V-WLC instance, use the license command. For more information, see the examples provided in this section.

### Supported in the following platforms:

- Service Platforms — NX 95XX, NX 96XX, VX 9000

### Syntax

```
vx9000 <MAC>
```

### Parameters

```
vx9000 <MAC>
```

|              |                                                                                                                           |
|--------------|---------------------------------------------------------------------------------------------------------------------------|
| vx9000 <MAC> | Configures a V-WLC and enters its configuration mode. The V-WLC configuration is the same as that of a normal controller. |
|--------------|---------------------------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config)#vx9000 11-22-33-44-55-66
nx9500-6C8809(config-device-11-22-33-44-55-66)#?
Device Mode commands:
 adopter-auto-provisioning-policy-lookup Use centralized auto-provisioning
```



|                           |                                                                                                                    |
|---------------------------|--------------------------------------------------------------------------------------------------------------------|
|                           | policy when adopted by another controller                                                                          |
| adoption                  | Adoption configuration                                                                                             |
| adoption-site             | Set system's adoption site                                                                                         |
| adoption-mode             | Configure the adoption mode for the access-points in this RF-Domain                                                |
| alias                     | Alias                                                                                                              |
| application-policy        | Application Policy configuration                                                                                   |
| area                      | Set name of area where the system is located                                                                       |
| arp                       | Address Resolution Protocol (ARP)                                                                                  |
| auto-learn                | Auto learning                                                                                                      |
| autogen-uniqueid          | Autogenerate a unique id                                                                                           |
| autoinstall               | Autoinstall settings                                                                                               |
| bluetooth-detection       | Detect Bluetooth devices using the Bluetooth USB module - there will be interference on 2.4 Ghz radio in wlan mode |
| bridge                    | Ethernet bridge                                                                                                    |
| captive-portal            | Captive portal                                                                                                     |
| cdp                       | Cisco Discovery Protocol                                                                                           |
| channel-list              | Configure channel list to be advertised to wireless clients                                                        |
| cluster                   | Cluster configuration                                                                                              |
| configuration-persistence | Enable persistence of configuration across reloads (startup configfile)                                            |
| contact                   | Configure the contact                                                                                              |
| controller                | WLAN controller configuration                                                                                      |
| country-code              | Configure the country of operation                                                                                 |
| critical-resource         | Critical Resource                                                                                                  |
| crypto                    | Encryption related commands                                                                                        |
| database                  | Database command                                                                                                   |
| device-upgrade            | Device firmware upgrade                                                                                            |
| dot1x                     | 802.1X                                                                                                             |
| dpi                       | Enable Deep-Packet-Inspection (Application Assurance)                                                              |
| dscp-mapping              | Configure IP DSCP to 802.1p priority mapping for untagged frames                                                   |
| email-notification        | Email notification configuration                                                                                   |
| enforce-version           | Check the firmware versions of devices before interoperating                                                       |
| environmental-sensor      | Environmental Sensors Configuration                                                                                |
| events                    | System event messages                                                                                              |
| export                    | Export a file                                                                                                      |
| file-sync                 | File sync between controller and adoptees                                                                          |
| floor                     | Set the floor within a area where the system is located                                                            |
| geo-coordinates           | Configure geo coordinates for this device                                                                          |
| gre                       | GRE protocol                                                                                                       |
| hostname                  | Set system's network name                                                                                          |
| http-analyze              | Specify HTTP-Analysis configuration                                                                                |
| interface                 | Select an interface to configure                                                                                   |
| ip                        | Internet Protocol (IP)                                                                                             |
| ipv6                      | Internet Protocol version 6 (IPv6)                                                                                 |
| l2tpv3                    | L2tpv3 protocol                                                                                                    |
| l3e-lite-table            | L3e lite Table                                                                                                     |
| layout-coordinates        | Configure layout coordinates for this device                                                                       |
| led                       | Turn LEDs on/off on the device                                                                                     |
| led-timeout               | Configure the time for the led to                                                                                  |

|                                    |                                                                                     |
|------------------------------------|-------------------------------------------------------------------------------------|
|                                    | turn off after the last radio state change                                          |
| legacy-auto-downgrade              | Enable device firmware to auto downgrade when other legacy devices are detected     |
| legacy-auto-update                 | Auto upgrade of legacy devices                                                      |
| license                            | License management command                                                          |
| lldp                               | Link Layer Discovery Protocol                                                       |
| load-balancing                     | Configure load balancing parameter                                                  |
| location                           | Configure the location                                                              |
| logging                            | Modify message logging facilities                                                   |
| mac-address-table                  | MAC Address Table                                                                   |
| mac-auth                           | 802.1X                                                                              |
| mac-name                           | Configure MAC address to name mappings                                              |
| management-server                  | Configure management server address                                                 |
| memory-profile                     | Memory profile to be used on the device                                             |
| meshpoint-device                   | Configure meshpoint device parameters                                               |
| meshpoint-monitor-interval         | Configure meshpoint monitoring interval                                             |
| min-misconfiguration-recovery-time | Check controller connectivity after configuration is received                       |
| mint                               | MiNT protocol                                                                       |
| mirror                             | Mirroring                                                                           |
| misconfiguration-recovery-time     | Check controller connectivity after configuration is received                       |
| mpact-server                       | MPACT server configuration                                                          |
| neighbor-inactivity-timeout        | Configure neighbor inactivity timeout                                               |
| neighbor-info-interval             | Configure neighbor information exchange interval                                    |
| no                                 | Negate a command or set its defaults                                                |
| noc                                | Configure the noc related setting                                                   |
| nsight                             | NSight                                                                              |
| ntp                                | Ntp server WORD                                                                     |
| offline-duration                   | Set duration for which a device remains unadopted before it generates offline event |
| override                           | Override a command                                                                  |
| override-wlan                      | Configure RF Domain level overrides for wlan                                        |
| power-config                       | Configure power mode                                                                |
| preferred-controller-group         | Controller group this system will prefer for adoption                               |
| preferred-tunnel-controller        | Tunnel Controller Name this system will prefer for tunneling extended vlan traffic  |
| radius                             | Configure device-level radius authentication parameters                             |
| raid                               | RAID                                                                                |
| remove-override                    | Remove configuration item override from the device (so profile value takes effect)  |
| rf-domain-manager                  | RF Domain Manager                                                                   |
| router                             | Dynamic routing                                                                     |
| rsa-key                            | Assign a RSA key to a service                                                       |
| sensor-server                      | AirDefense sensor server configuration                                              |
| slot                               | PCI expansion Slot                                                                  |
| spanning-tree                      | Spanning tree                                                                       |
| timezone                           | Configure the timezone                                                              |

|                       |                                                                               |
|-----------------------|-------------------------------------------------------------------------------|
| traffic-class-mapping | Configure IPv6 traffic class to 802.1p priority mapping for untagged frames   |
| trustpoint            | Assign a trustpoint to a service                                              |
| tunnel-controller     | Tunnel Controller group this controller belongs to                            |
| use                   | Set setting to use                                                            |
| vrrp                  | VRRP configuration                                                            |
| vrrp-state-check      | Publish interface via OSPF/BGP only if the interface VRRP state is not BACKUP |
| wep-shared-key-auth   | Enable support for 802.11 WEP shared key authentication                       |
| clrscr                | Clears the display screen                                                     |
| commit                | Commit all changes made in this session                                       |
| do                    | Run commands from Exec mode                                                   |
| end                   | End current mode and change to EXEC mode                                      |
| exit                  | End current mode and down to previous mode                                    |
| help                  | Description of the interactive help system                                    |
| revert                | Revert changes                                                                |
| service               | Service Commands                                                              |
| show                  | Show running system information                                               |
| write                 | Write running configuration to memory or terminal                             |

nx9500-6C8809(config-device-11-22-33-44-55-66)#

### Related Commands

|  |
|--|
|  |
|--|

# COMMON COMMANDS

## COMMON COMMANDS

---

This chapter describes the CLI commands common to the USER EXEC, PRIV EXEC, and GLOBAL CONFIG modes.

The PRIV EXEC command set contains commands available within the USER EXEC mode. Some commands can be entered in either mode. Commands entered in either the USER EXEC or PRIV EXEC mode are referred to as EXEC mode commands. If a user or privilege is not specified, the referenced command can be entered in either mode.

### common-commands

The following table summarizes the commands common to the User Exec, Priv Exec, Global Config modes, and all other configuration contexts:

*Table: Common Commands*

| Command              | Description                                                                           |
|----------------------|---------------------------------------------------------------------------------------|
| <code>clrscr</code>  | Clears the display screen                                                             |
| <code>commit</code>  | Commits (saves) changes made in the current session                                   |
| <code>exit</code>    | Ends and exits the current mode and moves to the PRIV EXEC mode                       |
| <code>help</code>    | Displays the interactive help system                                                  |
| <code>no</code>      | Negates a command or reverts values to their default settings                         |
| <code>revert</code>  | Reverts changes to their last saved configuration                                     |
| <code>service</code> | Invokes service commands to troubleshoot or debug (config-if) instance configurations |
| <code>show</code>    | Displays running system information                                                   |
| <code>write</code>   | Writes the system's running configuration to memory or terminal                       |

#### *clrscr*

Clears the screen and refreshes the prompt, irrespective of the mode

#### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### **Syntax**

```
clrscr
```

## Parameters

None

## Examples

The following example shows the terminal window or screen before the `clrscr` command is executed:

```
rfs4000-229D58#device-upgrade ?
 DEVICE-NAME Name/MAC address of device
 all Upgrade all devices
 ap650 Upgrade AP650 Device
 ap6522 Upgrade AP6522 Device
 ap6532 Upgrade AP6532 Device
 ap6562 Upgrade AP6562 Device
 ap71xx Upgrade AP7161 Device
 ap7502 Upgrade AP7502 Device
 ap7522 Upgrade AP7522 Device
 ap7532 Upgrade AP7532 Device
 ap7562 Upgrade AP7562 Device
 ap81xx Upgrade AP8163 Device
 ap8432 Upgrade AP8432 Device
 ap8533 Upgrade AP8533 Device
 cancel-upgrade Cancel upgrading the device
 load-image Load the device images to controller for device-upgrades
 rf-domain Upgrade all devices belonging to an RF Domain
 rfs4000 Upgrade RFS4010 Device
```

```
rfs4000-229D58#
```

The terminal window or screen after the `clrscr` command is executed:

```
rfs4000-229D58#
```

## *commit*

Commits changes made in the active session. Use the `commit` command to save and invoke settings entered during the current transaction.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
commit {write}{memory}
```

## Parameters

```
commit {write}{memory}
```

|        |                                                                                         |
|--------|-----------------------------------------------------------------------------------------|
| write  | Optional. Commits changes made in the current session                                   |
| memory | Optional. Writes to memory. This option ensures current changes persist across reboots. |

## Examples

```
nx9500-6C8809#commit write memory
[OK]
nx9500-6C8809#
```

## exit

The exit command works differently in the User Exec, Priv Exec, and Global Config modes. In the Global Config mode, it ends the current mode and moves to the previous mode, which is Priv Exec mode. The prompt changes from *(config)#* to *#*. When used in the Priv Exec and User Exec modes, the exit command ends the current session, and connection to the terminal device is terminated. If the current session has changes that have not been committed, the system will prompt you to either do a commit or a revert before terminating the session.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
exit
```

### Parameters

None

### Examples

```
nx9500-6C8809(config)#exit
nx9500-6C8809#
```

## help

Describes the interactive help system

Use this command to access the advanced help feature. Use "?" anytime at the command prompt to access the help topic

Two kinds of help are provided:

- Full help is available when ready to enter a command argument
- Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (for example 'show ve?').

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
help {search/show}
help {search <WORD>} {detailed/only-show/skip-no/skip-show}
```

### Parameters

```
help {search <WORD>} {detailed/only-show/skip-no/skip-show}
```

|               |                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| search <WORD> | Optional. Searches for CLI commands related to a specific target term <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specify a target term (for example, a feature or a configuration parameter). After specifying the term, select one of the following options: detailed, only-show, skip-no, or skip-show. The system displays information based on the option selected.</li> </ul> |
| detailed      | Optional. Searches and displays help strings in addition to mode and commands                                                                                                                                                                                                                                                                                                                   |
| only-show     | Optional. Displays only "show" commands. Does not display configuration commands.                                                                                                                                                                                                                                                                                                               |
| skip-no       | Optional. Displays only configuration commands. Does not display "no" commands                                                                                                                                                                                                                                                                                                                  |
| skip-show     | Optional. Displays only configuration commands. Does not display "show" commands                                                                                                                                                                                                                                                                                                                |

## Examples

```
nx9500-6C8809>help search crypto detailed
found more than 64 references, showing the first 64
```

```
Context : Command
Command : clear crypto ike sa (A.B.C.D|all)(|on DEVICE-NAME)
 \ Clear
 \ Encryption Module
 \ IKE SA
 \ Flush IKE SAs
 \ Flush IKE SAs for a given peer
 \ Flush all IKE SA
 \ On AP/Controller
 \ AP/Controller name

 : clear crypto ipsec sa(|on DEVICE-NAME)
 \ Clear
 \ Encryption Module
 \ IPsec database
 \ Flush IPsec SAs
 \ On AP/Controller
 \ AP/Controller name

 : crypto key export rsa WORD URL (passphrase WORD|) (background|) ...
 \ Encryption related commands
```

--More--

```
nx9500-6C8809>
nx9500-6C8809>help search crypto only-show
```

```
Context : Command
Command : show crypto cmp request status(|on DEVICE-NAME)
 : show crypto ike sa (version 1|version 2|)(peer A.B.C.D|) (detail...
 : show crypto ipsec sa (peer A.B.C.D|) (detail|) (|on DEVICE-NAME...
 : show crypto key rsa (|public-key-detail) (|on DEVICE-NAME)
 : show crypto pki trustpoints (WORD|all|)(|on DEVICE-NAME)
```

```
nx9500-6C8809>
```

```
nx9500-6C8809>help search service skip-show
found more than 64 references, showing the first 64
```

```
Context : Command
Command : service block-adopter-config-update
 : service clear adoption history(|on DEVICE-NAME)
 : service clear captive-portal-page-upload history (|(on DOMAIN-NA...
 : service clear command-history(|on DEVICE-NAME)
 : service clear device-upgrade history (|on DOMAIN-NAME)
 : service clear noc statistics
 : service clear reboot-history(|on DEVICE-NAME)
 : service clear unsanctioned aps (|on DEVICE-OR-DOMAIN-NAME)
 : service clear upgrade-history(|on DEVICE-NAME)
```

```

: service clear web-filter cache(|on DEVICE-NAME)
: service clear wireless ap statistics (|(AA-BB-CC-DD-EE-FF)) (|on...
: service clear wireless client statistics (|AA-BB-CC-DD-EE-FF) (|...
: service clear wireless controller-mobility-database
: service clear wireless dns-cache(|on DEVICE-OR-DOMAIN-NAME)
: service clear wireless radio statistics (|(DEVICE-NAME (<1-3>))...
: service clear wireless wlan statistics (|WLAN) (|on DEVICE-OR-DO...
: service clear xpath requests (<1-100000>)
: service show block-adopter-config-update
: service show captive-portal servers(|on DEVICE-NAME)
: service show captive-portal user-cache(|on DEVICE-NAME)
: service show cli
--More--

```

```

nx9500-6C8809>
nx9500-6C8809>help search mint only-show
Found 25 references for "mint"

```

```

Context : Command
Command : show debugging mint (|on DEVICE-OR-DOMAIN-NAME)
: show mint config(|on DEVICE-NAME)
: show mint dis (|details)(|on DEVICE-NAME)
: show mint id(|on DEVICE-NAME)
: show mint info(|on DEVICE-NAME)
: show mint known-adopters(|on DEVICE-NAME)
: show mint links (|details)(|on DEVICE-NAME)
: show mint lsp
: show mint lsp-db (|details AA.BB.CC.DD)(|on DEVICE-NAME)
: show mint mlcp history(|on DEVICE-NAME)
: show mint mlcp(|on DEVICE-NAME)
: show mint neighbors (|details)(|on DEVICE-NAME)
: show mint route(|on DEVICE-NAME)
: show mint stats(|on DEVICE-NAME)
: show mint tunnel-controller (|details)(|on DEVICE-NAME)
: show mint tunneled-vlans(|on DEVICE-NAME)
: show wireless mint client (|on DEVICE-OR-DOMAIN-NAME)
: show wireless mint client portal-candidates(|(DEVICE-NAME (<1-3...
: show wireless mint client statistics (|on DEVICE-OR-DOMAIN-NAME)...
: show wireless mint client statistics rf (|on DEVICE-OR-DOMAIN-NA...
: show wireless mint detail (|(DEVICE-NAME (<1-3>))) (|(filter {|...
: show wireless mint links (|on DEVICE-OR-DOMAIN-NAME)
: show wireless mint portal (|on DEVICE-OR-DOMAIN-NAME)
: show wireless mint portal statistics (|on DEVICE-OR-DOMAIN-NAME)...
: show wireless mint portal statistics rf (|on DEVICE-OR-DOMAIN-NA...
nx9500-6C8809>

```

*no*

Negates a command or sets its default. Though the `no` command is common to the User Exec, Priv Exec, and Global Config modes, it negates a different set of commands in each mode.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
no <PARAMETER>
```



## Parameters

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| no <PARAMETERS> | The no command is common across all configuration modes and sub modes. It resets or reverts settings based on the mode in which executed. For example, when executed in the AAA policy configuration mode, it allows you to reset or revert a specific AAA policy settings. Similarly, when executed in the global configuration mode, it only resets or reverts settings configured in the global configuration mode. |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Usage Guidelines

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Global Config mode: No command options

|                                    |                                                                  |
|------------------------------------|------------------------------------------------------------------|
| ap8432-070235(config)#no ?         |                                                                  |
| aaa-policy                         | Delete a aaa policy                                              |
| aaa-tacacs-policy                  | Delete a aaa tacacs policy                                       |
| alias                              | Alias                                                            |
| ap7522                             | Delete an AP7522 access point                                    |
| ap7532                             | Delete an AP7532 access point                                    |
| ap7562                             | Delete an AP7562 access point                                    |
| ap7602                             | Delete an AP7602 access point                                    |
| ap7612                             | Delete an AP7612 access point                                    |
| ap7622                             | Delete an AP7622 access point                                    |
| ap7632                             | Delete an AP7632 access point                                    |
| ap7662                             | Delete an AP7662 access point                                    |
| ap8432                             | Delete an AP8432 access point                                    |
| ap8533                             | Delete an AP8533 access point                                    |
| application                        | Delete an application                                            |
| application-group                  | Delete an application-group                                      |
| application-policy                 | Delete an application policy                                     |
| association-acl-policy             | Delete an association-acl policy                                 |
| auto-provisioning-policy           | Delete an auto-provisioning policy                               |
| bonjour-gw-discovery-policy        | Disable Bonjour Gateway discovery policy                         |
| bonjour-gw-forwarding-policy       | Disable Bonjour Gateway Forwarding policy                        |
| bonjour-gw-query-forwarding-policy | Disable Bonjour Gateway Query Forwarding policy                  |
| captive-portal                     | Delete a captive portal                                          |
| client-identity                    | Client identity (DHCP Device Fingerprinting)                     |
| client-identity-group              | Client identity group (DHCP Fingerprint Database)                |
| crypto-cmp-policy                  | CMP policy                                                       |
| customize                          | Restore the custom cli commands to default                       |
| device                             | Delete multiple devices                                          |
| device-categorization              | Delete device categorization object                              |
| dhcp-server-policy                 | DHCP server policy                                               |
| dhcpv6-server-policy               | DHCPv6 server related configuration                              |
| dns-whitelist                      | Delete a whitelist object                                        |
| event-system-policy                | Delete a event system policy                                     |
| ex3500-qos-class-map-policy        | Delete a ex3500 qos class-map policy                             |
| ex3500-qos-policy-map              | Delete a ex3500 qos policy-map                                   |
| firewall-policy                    | Configure firewall policy                                        |
| global-association-list            | Delete a global association list                                 |
| igmp-snoop-policy                  | Remove device onboard igmp snoop policy                          |
| inline-password-encryption         | Disable storing encryption key in the startup configuration file |
| ip                                 | Internet Protocol (IP)                                           |

|                                  |                                                                       |
|----------------------------------|-----------------------------------------------------------------------|
| ipv6                             | Internet Protocol version 6 (IPv6)                                    |
| ipv6-router-advertisement-policy | IPv6 Router Advertisement related configuration                       |
| l2tpv3                           | Negate a command or set its defaults                                  |
| mac                              | MAC configuration                                                     |
| management-policy                | Delete a management policy                                            |
| meshpoint                        | Delete a meshpoint object                                             |
| meshpoint-qos-policy             | Delete a mesh point QoS configuration policy                          |
| nac-list                         | Delete an network access control list                                 |
| nsight-policy                    | Delete a nsight policy                                                |
| passpoint-policy                 | Delete a passpoint configuration policy                               |
| password-encryption              | Disable password encryption in configuration                          |
| profile                          | Delete a profile and all its associated configuration                 |
| radio-qos-policy                 | Delete a radio QoS configuration policy                               |
| radius-group                     | Local radius server group configuration                               |
| radius-server-policy             | Remove device onboard radius policy                                   |
| radius-user-pool-policy          | Configure Radius User Pool                                            |
| rf-domain                        | Delete one or more RF-domains and all their associated configurations |
| roaming-assist-policy            | Delete a roaming-assist policy                                        |
| role-policy                      | Role based firewall policy                                            |
| routing-policy                   | Policy Based Routing Configuratio                                     |
| rtl-server-policy                | Delete a rtl server policy                                            |
| schedule-policy                  | Delete a schedule policy                                              |
| sensor-policy                    | Delete a sensor policy                                                |
| smart-rf-policy                  | Delete a smart-rf-policy                                              |
| url-filter                       | Delete a url filter                                                   |
| url-list                         | Delete a URL list                                                     |
| web-filter-policy                | Delete a web filter policy                                            |
| wips-policy                      | Delete a wips policy                                                  |
| wlan                             | Delete a wlan object                                                  |
| wlan-qos-policy                  | Delete a wireless lan QoS configuration policy                        |
| service                          | Service Commands                                                      |

ap8432-070235(config)#

Priv Exec mode: No command options

ap8432-070235(config)#exit

ap8432-070235#no ?

|                |                                                                  |
|----------------|------------------------------------------------------------------|
| adoption       | Reset adoption state of the device (& all devices adopted to it) |
| captive-portal | Captive portal commands                                          |
| crypto         | Encryption related commands                                      |
| debug          | Debugging functions                                              |
| logging        | Modify message logging facilities                                |
| page           | Toggle paging                                                    |
| service        | Service Commands                                                 |
| terminal       | Set terminal line parameters                                     |
| upgrade        | Remove a patch                                                   |
| wireless       | Wireless Configuration/Statistics commands                       |

ap8432-070235#

User Exec mode: No command options

ap8432-070235#disable

ap8432-070235>no ?

|          |                                                              |
|----------|--------------------------------------------------------------|
| adoption | Reset adoption state of the device (& all devices adopted to |
|----------|--------------------------------------------------------------|

```

it)
captive-portal Captive portal commands
crypto Encryption related commands
debug Debugging functions
logging Modify message logging facilities
page Toggle paging
service Service Commands
terminal Set terminal line parameters
wireless Wireless Configuration/Statistics commands

```

ap8432-070235>

### Related Commands

|    |                          |
|----|--------------------------|
| no | User Exec no command     |
| no | Priv Exec no command     |
| no | Global Config no command |

### revert

Reverts changes made, in the current session, to their last saved configuration

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
revert
```

#### Parameters

None

#### Examples

```

nx9500-6C8809revert
nx9500-6C8809

```

### service

Service commands are used to view and manage configurations. The service commands and their corresponding parameters vary from mode to mode. The *User Exec mode* and *Priv Exec mode* commands provide same functionalities with a few minor changes. The Global Config service command sets the size of history files. It also enables viewing the current mode's CLI tree.

This topic is organized into the following sections:

- [Syntax \(User Exec Mode\)](#)
- [Parameters \(User Exec Mode\)](#)
- [Syntax \(Priv Exec Mode\)](#)
- [Parameters \(Priv Exec Mode\)](#)

- 
- [Syntax - NX9XXX-Specific \(Privi Exec Mode\)](#)
  - [Parameters - NX9XXX-Specific \(Privi Exec Mode\)](#)
  - [Syntax \(Global Config Mode\)](#)
  - [Parameters \(Global Config Mode\)](#)
  - [Examples](#)

**Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

**Syntax (User Exec Mode)**

[Service Commands - Intro](#)

```
service [block-adopter-config-update|clear|cli-tables-skin|cluster|database|
delete-offline-aps|eguest|force-send-config|force-update-vm-stats|
```

```

guest-registration|load-balancing|load-ssh-authorized-keys|locator|nsight|radio|
radius|request-full-config-from-adopter|set|show|smart-rf|ssm|snmp|syslog|wireless]
service [block-adopter-config-update|request-full-config-from-adopter]
service eguest [remove-data|restore]
service eguest remove-data [deleted-devices|offline-for days <0-999>
{time <HH:MM:SS>}]
service eguest restore factory-default
service clear [adoption|captive-portal-page-upload|command-history|device-upgrade|
diag|dpi|file-sync|noc|reboot-history|unsanctioned|upgrade-history|virtual-machine-history|
web-filter|wireless|xpath]
service clear adoption history {on <DEVICE-NAME>}
service clear device-upgrade history {on <DOMAIN-NAME>}
service clear dpi [all|app|app-category] stats {on <DEVICE-OR-DOMAIN-NAME>}
service clear diag pkts
service clear file-sync history {on <DOMAIN-NAME>}
service clear captive-portal-page-upload history {on <DOMAIN-NAME>}
service clear [command-history|reboot-history|upgrade-history|virtual-machine-history]
{on <DEVICE-NAME>}
service clear noc statistics
service clear unsanctioned aps {on <DEVICE-OR-DOMAIN-NAME>}
service clear web-filter cache {on <DEVICE-NAME>}
service clear wireless [ap|client|controller-mobility-database|dns-cache|radio|wlan]
service clear wireless controller-mobility-database
service clear wireless [ap|client|controller-mobility-database|dns-cache|radio|wlan]
service clear wireless controller-mobility-database
service clear wireless [ap|client] statistics {<MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}
service clear wireless dns-cache on {(on <DEVICE-OR-DOMAIN-NAME>)}
service clear wireless radio statistics {<MAC/HOSTNAME>} {<1-3>}
{(on <DEVICE-OR-DOMAIN-NAME>)}
service clear wireless wlan statistics {<WLAN-NAME>} {(on <DEVICE-OR-DOMAIN-NAME>)}
service clear xpath requests {<1-10000>}
service cli-tables-skin [ansi|hashes|minimal|none|percent|stars|thick|thin|utf-8]
{grid}
service cluster force [active|configured-state|standby]
service database [authentication|start-shell]
service database authentication [create-user|delete-user]
service database authentication create-user username <USER-NAME> password <PASSWORD>
service database authentication delete-user username <USER-NAME>
service database start-shell
service delete-offline-aps [all|offline-for]
service delete-offline-aps offline-for days <0-999> {time <TIME>}
service force-send-config {on <DEVICE-OR-DOMAIN-NAME>}
service force-update-vm-stats {on <DEVICE-NAME>}
service guest-registration [backup|delete|export|import]
service guest-registration backup [delete|restore]
service guest-registration delete [all|email <EMAIL-ADD>|group <RAD-GROUP-NAME>|
mac <MAC>|mobile <MOBILE-NUMBER>|name <CLIENT-FULL-NAME>|non-social|

```

```

offline-for days <1-999>|otp-incomplete-for days <1-999>|social [facebook|google]|
wlan <WLAN-NAME>]
service guest-registration export format [csv|json] <DEST-URL>
{(rfdomain <DOMAIN-NAME>/time [1-Day/1-Month/1-Week/2-Hours/30-Mins/5-Hours/all]/
wlan <WLAN-NAME>)}
service guest-registration import format <JSON> <SOURCE-URL>
service load-balancing clear-client-capability [<MAC>|all] {on <DEVICE-NAME>}
service load-ssh-authorized-keys <PUBLIC-KEY> {on <DEVICE-NAME>}
service locator {<1-60>} {(on <DEVICE-NAME>)}
service nsight clear-offline [all|offline-for days <0-999> {time <TIME>}]
service radio <1-3> [adaptivity|channel-switch|dfs]
service radio <1-3> adaptivity
service radio <1-3> channel-switch <36-196> [160|20|40|80]
service radio <1-3> dfs simulator-radar [extension|primary]
service radius test [<IP>|<HOSTNAME>] [<WORD>|<PORT>]
service radius test [<IP>|<HOSTNAME>] <WORD> <USERNAME> <PASSWORD>
{wlan <WLAN-NAME> ssid <SSID>} {(on <DEVICE-NAME>)}
service radius test [<IP>|<HOSTNAME>] port <1024-65535> <WORD> <USERNAME> <PASSWORD>
{wlan <WLAN-NAME> ssid <SSID>} {(on <DEVICE-NAME>)}
service set validation-mode [full|partial] {on <DEVICE-NAME>}
service show [block-adopter-config-update|captive-portal|cli|client-identity-defaults|
command-history|configuration-revision|crash-info|dhcp-lease|diag|fast-switching|fib|
fib6|guest-registration|info|ip-access-list|mac-vendor|mem|mint|noc|nsight|pm|process|

```

```

reboot-history|rf-domain-manager|sites|snmp|ssh-authorized-keys|startup-log|sysinfo|
top|upgrade-history|virtual-machine-history|watch-dog|wireless|xpath-history]
service show block-adopter-config-update
service show captive-portal [log-internal|servers|user-cache]
service show captive-portal log-internal
service show captive-portal [servers|user-cache] {on <DEVICE-NAME>}
service show [cli|client-identity-defaults|configuration-revision|mac-vendor <OUI/MAC>|
noc diag|snmp session|xpath-history]
service show [command-history|crash-info|info|mem|process|reboot-history|startup-log|
ssh-authorized-keys|sysinfo|top|upgrade-history|watchdog] {on <DEVICE-NAME>}
service show ip-access-list wlan <WLAN-NAME> status {detail}
{on <DEVICE-OR-DOMAIN-NAME>}
service show dhcp-lease {<INTERFACE-NAME>/pppoe1/vlan <1-4094>/wwan1}
{on <DEVICE-NAME>}
service show diag [fds|led-status|pkts|psu|stats]
service show diag [fds|pkts]
service show diag [led-status|psu|stats] {on <DEVICE-NAME>}
service show fast-switching {on <DEVICE-NAME>}
service show [fib|fib6] {table-id <0-255>}
service show guest-registration [export-status|import-status|restore-status]
service show mint [adopted-devices {on <DEVICE-NAME>}|ports]
service show pm {history} {{on <DEVICE-NAME>}}
service show rf-domain-manager [diag|info] {<MAC/HOSTNAME>}
{{on <DEVICE-OR-DOMAIN-NAME>}}
service show sites
service show virtual-machine-history {on <DEVICE-NAME>}
service show wireless [aaa-stats|adaptivity-status|client|config-internal|
credential-cache|dns-cache|log-internal|meshpoint|neighbors|radar-status|
radio-internal|reference|stats-client|vlan-usage]
service show wireless [aaa-stats|adaptivity-status|credential-cache|dns-cache|
radar-status|vlan-usage] {on <DEVICE-NAME>}
service show wireless [config-internal|log-internal|neighbors]
service show wireless [client|meshpoint neighbor] proc [info|stats] {<MAC>}
{{on <DEVICE-OR-DOMAIN-NAME>}}
service show wireless radio-internal [radio1|radio2] <LINE>
service show wireless reference [channels|frame|handshake|mcs-rates|reason-codes|
status-codes]
service show wireless stats-client diag {<MAC/HOSTNAME>}
{{on <DEVICE-OR-DOMAIN-NAME>}}
service smart-rf [clear-config|clear-history|clear-interfering-aps|save-config]
service smart-rf clear-config {<MAC>/<DEVICE-NAME>/on <DOMAIN-NAME>}
service smart-rf [clear-history||clear-interfering-aps|save-config] {on <DOMAIN-NAME>}
service snmp sysoid wing5
service ssm [dump-core-snapshot|trace]
service ssm trace pattern <WORD> {on <DEVICE-NAME>}
service syslog test {level [<0-7>|alerts|critical|debugging|emergencies|errors|
informational|notifications|warnings]} {{on <DEVICE-NAME>}}
service wireless [client|dump-core-snapshot|meshpoint|qos|trace|unsanctioned|wips]
service wireless client [beacon-request|quiet-element|trigger-bss-transition|trigger-wnm]
service wireless client beacon-request <MAC> mode [active|passive|table]
ssid [<SSID>|any] channel-report [<CHANNEL-LIST>|none] {on <DEVICE-NAME>}
service wireless client trigger-bss-transition mac <MAC> {timeout <0-65535>}
{url <URL>} {on <DEVICE-OR-DOMAIN-NAME>}
service wireless client trigger-wnm mac <MAC> type
[deauth-imminent|subscription-remediation] {uri <WORD>}
service wireless dump-core-snapshot
service wireless meshpoint zl <MESHPOINT-NAME> [on <DEVICE-NAME>]
{<ARGS>/timeout <1-65535>}
service wireless qos delete-tspec <MAC> tid <0-7>
service wireless trace pattern <WORD> {on <DEVICE-NAME>}
service wireless unsanctioned ap air-terminate <MAC> {on <DOMAIN-NAME>}
service wireless wips [clear-client-blacklist|clear-event-history|dump-managed-config]
service wireless wips clear-client-blacklist [all|mac <MAC>]
service wireless wips clear-event-history {on <DEVICE-OR-DOMAIN-NAME>}

```

## Parameters (User Exec Mode)

### Service Commands - Intro

```
service [block-adopter-config-update|request-full-config-from-adopter]
```

|                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| block-adopter-config-update      | Blocks the configuration updates pushed from the NOC (Network Operations Center) server to adopted devices                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| request-full-config-from-adopter | Configures a request for full configuration updates from the adopter device<br>In an HM (hierarchically managed) network devices are deployed in two levels. The first level consists of the NOC controllers. The second level consists of the site controllers that can be grouped to form clusters. The NOC controllers adopt and manage the site controllers. Access points within the network are adopted and managed by the site controllers. The adopted devices (Access Points and site controllers) are referred to as the adoptee. The devices adopting the adoptee are the 'adopters'. |

```
service clear adoption history {on <DEVICE-NAME>}
```

|                        |                                                                                                                                                                                                     |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| clear adoption history | Clears adoption history on this device and its adopted Access Points                                                                                                                                |
| on <DEVICE-NAME>       | Optional. Clears adoption history on a specified device <ul style="list-style-type: none"><li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li></ul> |

```
service clear device-upgrade history {on <DOMAIN-NAME>}
```

|                              |                                                                                                                                                                          |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| clear device-upgrade history | Clears device upgrade history                                                                                                                                            |
| on <DOMAIN-NAME>             | Optional. Clears all firmware upgrade history on a specified RF Domain <ul style="list-style-type: none"><li>&lt;DOMAIN-NAME&gt; - Specify the RF Domain name.</li></ul> |

```
service clear diag pkts
```

|                 |                                                                                                                                                                                                                                                                                                                                                 |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| clear diag pkts | Clears the looped packets queue logged by the dataplane. The dataplane logs up to 16 looped packets at a time in a separate queue, which has to be manually cleared to make space for new packet logging.<br>For more information on viewing logged looped packet information execute the <b>service &gt; show &gt; diag &gt; pkts</b> command. |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
service clear dpi [all|app|app-category] stats {on <DEVICE-OR-DOMAIN-NAME>}
```



|                              |                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| clear dpi                    | Clears DPI (Deep Packet Inspection) statistics<br>When enabled, DPI allows application and/or application category recognition. The DPI statistics are maintained by the system for every hit registered by the DPI engine.                                                                                                            |
| [all app app-category] stats | Use the following filter options to clear all or specific DPI statistics: <ul style="list-style-type: none"> <li>• all – Clears all DPI related (application and app-category) statistics</li> <li>• app – Clears only application related statistics</li> <li>• app-category – Clears only app-category related statistics</li> </ul> |
| on <DEVICE-OR-DOMAIN-NAME>   | Optional. Clears DPI statistics based on the parameters passed on a specified device or RF Domain <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the access point, controller, service platform, or RF Domain.</li> </ul>                                                                |

```
service eguest remove-data [deleted-devices|offline-for days <0-999> {time <HH:MM:SS>}]
```

|                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| service eguests                               | Enables ExtremeGuest (EGuest) server data maintenance                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| remove-data                                   | Removes offline and/or deleted devices from the ExtremeGuest server database<br><br><b>Note:</b> When enabled, the device configuration and database collection is removed permanently.<br><br><b>Note:</b> If a controller is removed, then its adopted APs are also removed,                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| deleted-devices                               | Removes deleted devices                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| offline-for days <0-999><br>{time <HH:MM:SS>} | Removes offline devices from the EGuest server database. Offline devices are devices that have not been reporting to the EGuest server for a specified number of days. Use this option to configure that threshold value. Devices that have not reported to the EGuest server for the number of days specified here are considered to be offline and removed. <ul style="list-style-type: none"> <li>• days &lt;0-999&gt; – Specify the threshold, in days, from 0 - 999.</li> <li>• time &lt;HH:MM:SS&gt; – Option. In addition to the number of days, you can also specify the time in hours, minutes, and seconds. If specified, a device is removed if it has not reported to the server for the specified number of days and time.</li> </ul> |

```
service eguest restore factory-default
```

|                         |                                                                                                                                                                                                                                                                                |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| eguest                  | Enables EGuest server data maintenance                                                                                                                                                                                                                                         |
| restore factory-default | Reinitializes the EGuest server to factory-default settings. Use this option to stop the EGuest server and database.<br><br><b>Note:</b> Extreme caution is recommended, as this command deletes data related to EGuest server and database. Debug log files are also deleted. |

```
service clear file-sync history {on <DOMAIN-NAME>}
```

|                         |                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| clear file-sync history | Clears client-bridge certificate synchronization statistics<br>When an AP 6522/AP 6562 access point is configured as a client bridge, the EAP-TLS X.509 (PKCS#12) certificate is synchronized between the staging-controller and adoptee AP 6522/AP 6562 client-bridge access points. This command allows you to clear client-bridge certificate synchronization statistics. |
| on <DOMAIN-NAME>        | Optional. Clears file synchronization history on all devices within a specified RF Domain <ul style="list-style-type: none"> <li>• &lt;DOMAIN-NAME&gt; – Specify the RF Domain name.</li> </ul>                                                                                                                                                                              |

```
service clear captive-portal-page-upload history {on <DOMAIN-NAME>}
```

|                                          |                                                                                                                                                                                    |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| clear captive-portal-page-upload history | Clears captive portal page upload history                                                                                                                                          |
| on <DOMAIN-NAME>                         | Optional. Clears captive portal page upload history on a specified RF Domain <ul style="list-style-type: none"> <li>• &lt;DOMAIN-NAME&gt; – Specify the RF Domain name.</li> </ul> |

```
service clear [command-history|reboot-history|upgrade-history|virtual-machine-history] {on <DEVICE-NAME>}
```

|                                                        |                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| clear [command-history reboot-history upgrade-history] | Clears command history, reboot history, and/or device upgrade history                                                                                                                                                                                                                                                                 |
| clear virtual-machine-history                          | Clears virtual-machine history on the logged device or a specified device<br>This command is applicable only on the NX 95XX series service platforms.                                                                                                                                                                                 |
| on <DEVICE-NAME>                                       | Optional. Clears history on a specified device <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform</li> </ul> <p><b>Note:</b> When executing the clear virtual-machine-history command, provide the name of the service platform running the VMs.</p> |

```
service clear noc statistics
```

|                      |                                           |
|----------------------|-------------------------------------------|
| clear noc statistics | Clears NOC applicable statistics counters |
|----------------------|-------------------------------------------|

```
service clear unsanctioned aps {on <DEVICE-OR-DOMAIN-NAME>}
```

|                            |                                                                                                                                                                                                                                                       |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| clear unsanctioned aps     | Clears the list of unsanctioned APs                                                                                                                                                                                                                   |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Clears the list of unsanctioned APs on a specified device or RF Domain <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> |

```
service clear wireless [ap|client] {<MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}
```

|                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| clear wireless [ap client] statistics | <p>Clears wireless statistics counters based on the parameters passed</p> <ul style="list-style-type: none"> <li>• ap statistics – Clears applicable AP statistics counters</li> <li>• client statistics – Clears applicable wireless client statistics counters</li> </ul>                                                                                                                                                                                             |
| <MAC> {on <DEVICE-OR-DOMAIN-NAME>}    | <p>The following keywords are common to the 'ap' and 'client' parameters:</p> <ul style="list-style-type: none"> <li>• &lt;MAC&gt; – Optional. Clears statistics counters for a specified AP or client. Specify the AP/client MAC address.</li> <li>• on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Clears AP/client statistics counters on a specified device or RF Domain. Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> |

service clear wireless controller-mobility-database

|                                             |                                                  |
|---------------------------------------------|--------------------------------------------------|
| clear wireless controller-mobility-database | Clears the controller assisted mobility database |
|---------------------------------------------|--------------------------------------------------|

service clear web-filter cache {on <DEVICE-NAME>}

|                        |                                                                                                                                                                                                                       |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| clear web-filter cache | Clears the cache used for Web filtering                                                                                                                                                                               |
| on <DEVICE-NAME>       | <p>Optional. Clears the Web filtering cache on a specified device</p> <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

service clear wireless radio statistics {<MAC/HOSTNAME> {<1-3>}}  
{(on <DEVICE-OR-DOMAIN-NAME>)}

|                                 |                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| clear wireless radio statistics | Clears applicable wireless radio statistics counters                                                                                                                                                                                                                                                                               |
| <MAC/HOSTNAME> <1-3>            | <p>Optional. Specify the MAC address or hostname of the radio, or append the interface number to form the radio ID in the AA-BB-CC-DD-EE-FF:RX or HOSTNAME:RX format.</p> <ul style="list-style-type: none"> <li>• &lt;1-3&gt; – Optional. Specify the radio interface index, if not specified as part of the radio ID.</li> </ul> |
| on <DEVICE-OR-DOMAIN-NAME>      | <p>Optional. This is a recursive parameter, which clears wireless radio statistics on a specified device or RF Domain.</p> <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul>                                    |

service clear wireless wlan statistics {<WLAN-NAME>} {(on <DEVICE-OR-DOMAIN-NAME>)}

|                                |                                                                                                                                                                                                                                                                                       |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| clear wireless wlan statistics | Clears WLAN statistics counters                                                                                                                                                                                                                                                       |
| <WLAN-NAME>                    | Optional. Clears statistics counters on a specified WLAN. Specify the WLAN name.                                                                                                                                                                                                      |
| on <DEVICE-OR-DOMAIN-NAME>     | <p>Optional. This is a recursive parameter, which clears WLAN statistics on a specified device or RF Domain.</p> <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> |

service clear xpath requests {<1-10000>}

|             |                                                                                                                                                                                                                                                                            |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| clear xpath | Clears XPATH related information                                                                                                                                                                                                                                           |
| requests    | Clears pending XPATH get requests                                                                                                                                                                                                                                          |
| <1-100000>  | Optional. Specifies the session number (cookie from show sessions) <ul style="list-style-type: none"> <li>• &lt;1-100000&gt; - Specify the session number from 1 - 100000.</li> </ul> <p><b>Note:</b> Omits clearing the current session's pending XPATH get requests.</p> |

```
service cli-tables-skin [ansi|hashes|minimal|none|percent|stars|thick|thin|utf-8]
{grid}
```

|                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cli-tables-skin [ansi hashes minimal none percent stars thick thin utf-8] | <p>Selects a formatting layout or skin for CLI tabular outputs</p> <ul style="list-style-type: none"> <li>• ansi - Uses ANSI characters for borders</li> <li>• hashes - Uses hashes (#) for borders</li> <li>• minimal - Uses one horizontal line between title and data rows</li> <li>• none - Displays space separated items with no decoration</li> <li>• percent - Uses the percent sign (%) for borders</li> <li>• stars - Uses asterisks (*) for borders</li> <li>• thick - Uses thick lines for borders</li> <li>• thin - Uses thin lines for borders</li> <li>• utf-8 - Uses UTF-8 characters for borders</li> </ul> |
| grid                                                                      | Optional. Uses a complete grid instead of just title lines                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

```
service cluster force [active|configured-state|standby]
```

|                  |                                                                             |
|------------------|-----------------------------------------------------------------------------|
| cluster          | Enables cluster protocol management                                         |
| force            | Forces action commands on a cluster (active, configured-state, and standby) |
| active           | Changes the cluster run status to active                                    |
| configured-state | Restores a cluster to the configured state                                  |
| standby          | Changes the cluster run status to standby                                   |

```
service database authentication create-user username <USER-NAME> password <PASSWORD>
```

|                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| database                                                            | Performs database related actions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| authentication create-user username <USER-NAME> password <PASSWORD> | <p>Creates users having access rights to the database. Execute this command on the database host. However, before creating users, on the database, generate the database keyfile. For more information on generating the keyfile, see <a href="#">database</a> (user exec mode).</p> <ul style="list-style-type: none"> <li>• username &lt;USER-NAME&gt; - Configures database username <ul style="list-style-type: none"> <li>• password &lt;PASSWORD&gt; - Configures a password for the username specified above</li> </ul> </li> </ul> <p>In the database-policy ensure that authentication is enabled and username and password is configured. The database-client-policy also should have the same username and password configured. For more information on database-policy and database-client-policy, see <a href="#">database-policy</a> and <a href="#">database-client-policy</a> (global config mode).</p> |

```
service database authentication delete-user username <USER-NAME>
```

|                                                          |                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| database                                                 | Performs database related actions<br>This command is supported only on the NX 95XX, NX 96XX, and VX 9000 platforms.                                                                                                                                                                                                                              |
| database authentication delete-user username <USER-NAME> | Deletes the username requires to access rights the captive-portal/NSight database <ul style="list-style-type: none"> <li>username &lt;USER-NAME&gt; – Deletes the username identified by the &lt;USER-NAME&gt; keyword</li> </ul> <p>Once deleted, the database cannot be accessed using the specified combination of username and password.</p> |

`service database start-shell`

|             |                                                                                                                     |
|-------------|---------------------------------------------------------------------------------------------------------------------|
| database    | Performs database related actions<br>This command is supported only on the NX 95XX, NX 96XX, and VX 9000 platforms. |
| start-shell | Starts the database shell                                                                                           |

`service delete-offline-aps all`

|                        |                                    |
|------------------------|------------------------------------|
| delete-offline-aps all | Deletes all off-line Access Points |
|------------------------|------------------------------------|

`service delete-offline-aps offline-for days <0-999> {time <TIME>}`

|                    |                                                                                                                                                                                                                 |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| delete-offline-aps | Deletes Access Points that have been off-line for a specified number of days and time period                                                                                                                    |
| day <0-999>        | Specifies the number of days an Access Point stays off-line to be deleted <ul style="list-style-type: none"> <li>&lt;0-999&gt; – Specify the number of off-line days from 0 - 999.</li> </ul>                   |
| time <TIME>        | Optional. Specifies the off-line time period. Access Points off-line for this period of time are deleted. <ul style="list-style-type: none"> <li>&lt;TIME&gt; – Specify the time in HH:MM:SS format.</li> </ul> |

`service force-send-config {on <DEVICE-OR-DOMAIN-NAME>}`

|                            |                                                                                                                                                                                                                                                                           |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| force-send-config          | Forces pushes configuration to device(s)                                                                                                                                                                                                                                  |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Pushes configuration to a specified device or all devices in a specified RF Domain <ul style="list-style-type: none"> <li>&lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> |

`service force-update-vm-stats {on <DEVICE-NAME>}`

|                       |                                                                                                                                                              |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| force-update-vm-stats | Forcefully pushes VM statistics on to the NOC                                                                                                                |
| on <DEVICE-NAME>      | Optional. Executes the command on a specified device <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; – Specify the name of the device.</li> </ul> |

`service guest-registration backup [delete|restore]`

```
service guest-registration
backup [delete|restore]
```

Deletes or restores all guest registration backup snapshots based on the parameter passed

- delete – Deletes all guest registration backup snapshots
- restores – Restores all guest registration backup snapshots

**Note:** To view the status of the restore process, use the **service > show > guest-registration > restore-status** command.

```
service guest-registration delete [all|email <EMAIL-ADD>|group <RAD-GROUP-NAME>|
mac <MAC>|mobile <MOBILE-NUMBER>|name <CLIENT-FULL-NAME>|non-social|
offline-for days <1-999>|wlan <WLAN-NAME>|otp-incomplete-for days <1-999>|
social [facebook|google]]
```

```
service guest-registration
delete
```

Deletes a specified user or all user records from the guest-registration database  
To delete a specific user, use one of the following options as an identification parameter: email, group, mac, mobile number, name, offline-for, wlan, otp-incomplete-for, or social.

```
[all|email <EMAIL-ADD>|group <RAD-GROUP-NAME>|mac <MAC>|mobile <MOBILE-NUMBER>|name <CLIENT-FULL-NAME>]|non-social|
offline-for days <1-999>|wlan <WLAN-NAME>|otp-incomplete-for days <1-999>|
social [facebook|google]
```

Following are the user filtering options: The user identified by one of the following parameters is deleted from the guest-registration database.

- email <EMAIL-ADD> – Identifies user by the e-mail address
  - <EMAIL-ADD> – Provide the user’s e-mail address.
- mac <MAC> – Identifies user by the MAC address
  - <MAC> – Provide the user’s MAC address.
- group <RAD-GROUP-NAME> – Identifies users by their RADIUS group association
  - <RAD-GROUP-NAME> – Specify the RADIUS group name.
- mobile <MOBILE-NUMBER> – Identifies user by the registered mobile number
  - <MOBILE-NUMBER> – Provide the user’s mobile number.
- name <CLIENT-FULL-NAME> – Identifies user by the registered full name
  - <CLIENT-FULL-NAME> – Provide the user’s full name.
- non-social – Identifies users that have not registered through social authentication
- offline-for days <1-999> – Filters users who have not accessed the network for a specified number of days
  - days <1-999> – Specify the number of days from 1 - 999.
- wlan <WLAN-NAME> – Identifies users accessing a specified WLAN
  - <WLAN-NAME> – Specify the WLAN name.
- otp-incomplete-for days <1-999> – Identifies records of users that have not used their OTP (one-time-password) to complete registration within a specified number of days
  - days <1-999> – Specify the number of days from 1 - 999.
- social [facebook|google] – Identifies users using either Facebook or Google credentials to access the network
  - facebook – Identifies users using Facebook authentication
  - google – Identifies users using Google authentication

```
service guest-registration export format [csv|json] <DEST-URL> {(rfdomain <DOMAIN-NAME>|
time [1-Day|1-Month|1-Week|2-Hours|30-Mins|5-Hours|all]|wlan <WLAN-NAME>)}
```

|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| service guest-registration export                       | Exports guest registration user data files in the CSV (Comma-Separated Values) or JSON (JavaScript Object Notation) format<br>Use the 'rfdomain', 'wlan', and 'time' options to filter users for a specified RF Domain, WLAN, and/or time period. These are recursive parameters and you can apply all or any of these three filters.                                                                                                                                                                                                                                                                                                                      |
| format [csv json]                                       | Specifies the file format. The options are: <ul style="list-style-type: none"> <li>• csv – Exports user data files in the CSV format</li> <li>• json – Exports user data files in the JSON format</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <DEST-URL>                                              | Configures the destination URL. The files are exported to the specified location. Both IPv4 and IPv6 address formats are supported. <ul style="list-style-type: none"> <li>• IPv4 URLs: <pre> tftp://&lt;hostname IP&gt;[:port]/path/file  ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IP&gt;[:port]/path/file  sftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IP&gt;[:port]/path/file </pre> </li> <li>• IPv6 URLs: <pre> tftp://&lt;hostname [IPv6]&gt;[:port]/path/file  ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname [IPv6]&gt;[:port]/path/file  sftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname [IPv6]&gt;[:port]/path/file </pre> </li> </ul> |
| rfdomain <DOMAIN-NAME>                                  | Optional. Filters user data based on RF Domain name. Only the filtered data are exported. <ul style="list-style-type: none"> <li>• &lt;DOMAIN-NAME&gt; – Specify the RF Domain name.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| wlan <WLAN-NAME>                                        | Optional. Filters user data based on WLAN name. Only the filtered data are exported. <ul style="list-style-type: none"> <li>• &lt;WLAN-NAME&gt; – Specify the WLAN name.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| time [1-Day 1-Month 1-Week 2-Hours 30-Mins 5-Hours all] | Optional. Filters user data for a specified time period. Only the filtered data are exported. <ul style="list-style-type: none"> <li>• 1-Day – Filters and exports previous day's data</li> <li>• 1-Month – Filters and exports previous month's data</li> <li>• 1-Week – Filters and exports previous week's data</li> <li>• 2-Hours – Filters and exports last 2 hours data</li> <li>• 30-Mins – Filters and exports last 30 minutes data</li> <li>• 5-Hours – Filters and exports last 5 hours data</li> <li>• all – Exports the entire database</li> </ul>                                                                                             |

```
service guest-registration import format json <SOURCE-URL>
```

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| service guest-registration import | Imports user data from a specified location                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| format json                       | Specifies the file format <ul style="list-style-type: none"> <li>json – Imports user data files in the JSON format</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <SOURCE-URL>                      | Configures the Source URL. The files are imported from the specified location. Both IPv4 and IPv6 address formats are supported. <ul style="list-style-type: none"> <li>IPv4 URLs: <pre>tftp://&lt;hostname IP&gt;[:port]/path/file</pre> <pre>ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IP&gt;[:port]/path/file</pre> <pre>sftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IP&gt;[:port]/path/file</pre> </li> <li>IPv6 URLs: <pre>tftp://&lt;hostname [IPv6]&gt;[:port]/path/file</pre> <pre>ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname [IPv6]&gt;[:port]/path/file</pre> <pre>sftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname [IPv6]&gt;[:port]/path/file</pre> </li> </ul> |

```
service load-balancing clear-client-capability [<MAC>|all] {on <DEVICE-NAME>}
```

|                                     |                                                                                                                                                                                                                                                                                                           |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| load-balancing                      | Enables wireless load balancing by clearing client capability records                                                                                                                                                                                                                                     |
| clear-client-capability [<MAC> all] | Clears a specified client or all client capability records <ul style="list-style-type: none"> <li>&lt;MAC&gt; – Clears capability records of a specified client. Specify the client's MAC address in the AA-BB-CC-DD-EE-FF format.</li> <li>all – Clears the capability records of all clients</li> </ul> |
| on <DEVICE-NAME>                    | Optional. Clears client capability records on a specified device <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul>                                                                                            |

```
service load-ssh-authorized-keys <PUBLIC-KEY> {on <DEVICE-NAME>}
```

|                          |                                                                                                                                                                                                              |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| load-ssh-authorized-keys | Loads SSH public (client) key on a device                                                                                                                                                                    |
| <PUBLIC-KEY>             | Enter the public key. The public key should be in the OpenSSH rsa/dsa format.                                                                                                                                |
| on <DEVICE-NAME>         | Optional. Loads the specified public key on a specified device <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
service locator {<1-60>} {(on <DEVICE-NAME>)}
```

|                  |                                                                                                                                                                                                                                                                                                                                           |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| locator          | Enables LEDs                                                                                                                                                                                                                                                                                                                              |
| <1-60>           | Sets LED flashing time from 1 - 60 seconds.                                                                                                                                                                                                                                                                                               |
| on <DEVICE-NAME> | The following keyword is recursive and common to the <1-60> parameter: <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; – Optional. Enables LEDs on a specified device <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; – Specify name of the AP, wireless controller, or service platform.</li> </ul> </li> </ul> |

```
service nsight clear-offline [all|offline-for days <0-999> {time <TIME>}]
```



|                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>nsight clear-offline [all offline-for days &lt;0-999&gt; {time &lt;TIME&gt;}]</pre> | <p>Clears NSight data received from offline controllers, based on the parameters passed. Select one of the following options:</p> <ul style="list-style-type: none"> <li>all – Clears NSight data received from all offline controllers</li> <li>offline-for days &lt;0-999&gt; time &lt;TIME&gt; – Clears NSight data received from controllers that have been offline for a specified time period <ul style="list-style-type: none"> <li>days &lt;0-999&gt; – Specifies the number of days controllers have been offline <ul style="list-style-type: none"> <li>&lt;0-999&gt; – Specify the number of days from 0 - 999 days. Select “0” to identify controllers offline less than 24 hours.</li> <li>time &lt;TIME&gt; – Optional. Specifies the total time for which controllers have been offline <ul style="list-style-type: none"> <li>&lt;TIME&gt; – Specify the time in HH:MM:SS format.</li> </ul> </li> </ul> </li> </ul> </li> </ul> <p><b>Note:</b> This command is applicable only to the NX 95XX, NX 96XX, and VX 9000 platforms.</p> |
|------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
service radio <1-3> adaptivity
```

|                              |                                                                                                                                        |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <pre>radio &lt;1-3&gt;</pre> | <p>Configures radio parameters</p> <ul style="list-style-type: none"> <li>&lt;1-3&gt; – Specify the radio index from 1 - 3.</li> </ul> |
| <pre>adaptivity</pre>        | <p>Simulates the presence of interference on the current channel</p>                                                                   |

```
service radio <1-3> channel-switch <36-196> [160|20|40|80|80-80]
```

|                                                               |                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>radio &lt;1-3&gt;</pre>                                  | <p>Configures radio parameters</p> <ul style="list-style-type: none"> <li>&lt;1-3&gt; – Specify the radio index from 1 - 3.</li> </ul>                                                                                                                                       |
| <pre>channel-switch &lt;36-196&gt; [160 20 40 80 80-80]</pre> | <p>Enables channel switching</p> <ul style="list-style-type: none"> <li>&lt;36-196&gt; – Specifies the channel to switch to from 36 - 196.</li> <li>160 20 40 80 80-80] – Specifies the bandwidth for the above specified channel. Select the appropriate option.</li> </ul> |

```
service radio <1-3> dfs simulate-radar [extension|primary]
```

|                                               |                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>radio &lt;1-3&gt;</pre>                  | <p>Configures radio parameters</p> <ul style="list-style-type: none"> <li>&lt;1-3&gt; – Specify the radio index from 1 - 3.</li> </ul>                                                                                                                                                                          |
| <pre>dfs</pre>                                | <p>Enables DFS (Dynamic Frequency Selection )</p>                                                                                                                                                                                                                                                               |
| <pre>simulate-radar [extension primary]</pre> | <p>Simulates the presence of a radar on a channel. Select the channel type from the following options:</p> <ul style="list-style-type: none"> <li>extension – Simulates a radar on the radio's current extension channel</li> <li>primary – Simulates a radar on the radio's current primary channel</li> </ul> |

```
service radius test [<IP>|<HOSTNAME>] <WORD> <USERNAME> <PASSWORD>
{wlan <WLAN-NAME> ssid <SSID>} {(on <DEVICE-NAME>)}
```

|                                 |                                                                                                                                                                                                                                                                       |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| radius test                     | Tests RADIUS server's account. This command sends an access-request packet to the RADIUS server. Use this command to confirm time and data/bandwidth parameters for valid wireless clients.<br>test - Tests the RADIUS server's account with user provided parameters |
| [<IP> <HOSTNAME>]               | Sets the RADIUS server's IP address or hostname <ul style="list-style-type: none"> <li>• &lt;IP&gt; - Specifies the RADIUS server's IP address</li> <li>• &lt;HOSTNAME&gt; - Specifies the RADIUS server's hostname</li> </ul>                                        |
| <WORD>                          | Specify the RADIUS server's shared secret.                                                                                                                                                                                                                            |
| <USERNAME>                      | Specify username for authentication.                                                                                                                                                                                                                                  |
| <PASSWORD>                      | Specify the password.                                                                                                                                                                                                                                                 |
| wlan <WLAN-NAME><br>ssid <SSID> | Optional. Tests the RADIUS server on the local WLAN. Specify the local WLAN name. <ul style="list-style-type: none"> <li>• ssid &lt;SSID&gt; - Specify the WLAN SSID.</li> </ul>                                                                                      |
| on <DEVICE-NAME>                | Optional. This is a recursive parameter also applicable to the WLAN parameter. Performs tests on a specified device <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul>   |

```
service radius test [<IP>|<HOSTNAME>] <PORT> <1024-65535> <WORD> <USERNAME>
<PASSWORD> {wlan <WLAN-NAME> ssid <SSID>} {(on <DEVICE-NAME>)}
```

|                                 |                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| radius test                     | Tests a RADIUS server's account. This command sends an access-request packet to the RADIUS server. Use this command to confirm time and data/bandwidth parameters for valid wireless clients. <ul style="list-style-type: none"> <li>• test - Tests the RADIUS server's account with user provided parameters</li> </ul> |
| [<IP> <HOSTNAME>]               | Sets the IP address or hostname of the RADIUS server <ul style="list-style-type: none"> <li>• &lt;IP&gt; - Specify the RADIUS server's IP address.</li> <li>• &lt;HOSTNAME&gt; - Specify the RADIUS server's hostname.</li> </ul>                                                                                        |
| <PORT> <1024-65535>             | Specify the RADIUS server port from 1024 - 65535. The default port is 1812.                                                                                                                                                                                                                                              |
| <WORD>                          | Specify the RADIUS server's shared secret.                                                                                                                                                                                                                                                                               |
| <USERNAME>                      | Specify username for authentication.                                                                                                                                                                                                                                                                                     |
| <PASSWORD>                      | Specify the password.                                                                                                                                                                                                                                                                                                    |
| wlan <WLAN-NAME><br>ssid <SSID> | Optional. Tests the RADIUS server on the local WLAN. Specify the local WLAN name. <ul style="list-style-type: none"> <li>• ssid &lt;SSID&gt; - Specify WLAN SSID.</li> </ul>                                                                                                                                             |
| on <DEVICE-NAME>                | Optional. This is a recursive parameter also applicable to the WLAN parameter. Performs tests on a specified device <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul>                                                      |

```
service set validation-mode [full|partial] {on <DEVICE-NAME>}
```

|                                |                                                                                                                                                                                                                                   |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| set                            | Sets the validation mode for running configuration validation                                                                                                                                                                     |
| validation-mode [full partial] | Sets the validation mode <ul style="list-style-type: none"> <li>• full – Performs a full configuration validation</li> <li>• partial – Performs a partial configuration validation</li> </ul>                                     |
| on <DEVICE-NAME>               | Optional. Performs full or partial configuration validation on a specified device <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

`service show block-adopter-conflict-update`

|                             |                                                                   |
|-----------------------------|-------------------------------------------------------------------|
| show                        | Displays running system statistics based on the parameters passed |
| block-adopter-config-update | Displays NOC configuration blocking status                        |

`service show captive-portal log-internal`

|                |                                                                                  |
|----------------|----------------------------------------------------------------------------------|
| show           | Displays running system statistics based on the parameters passed                |
| captive-portal | Displays captive portal information                                              |
| log-internal   | Displays recent captive portal debug logs (information and above severity level) |

`service show captive-portal [servers|user-cache] {on <DEVICE-NAME>}`

|                  |                                                                                                                                                                                                                                    |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show             | Displays running system statistics based on the parameters passed                                                                                                                                                                  |
| captive-portal   | Displays captive portal information                                                                                                                                                                                                |
| servers          | Displays server information for active captive portals                                                                                                                                                                             |
| user-cache       | Displays cached user details for a captive portal                                                                                                                                                                                  |
| on <DEVICE-NAME> | Optional. Displays server information or cached user details on a specified device <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

`service show [cli|client-identity-defaults|configuration-revision|mac-user-import-status|mac-vendor <OUI/MAC>|noc diag|snmp session|xpath-history]`

|                          |                                                                                                                                                                                                                                                                                                                                         |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show                     | Displays running system statistics based on the parameters passed                                                                                                                                                                                                                                                                       |
| cli                      | Displays CLI tree of the current mode                                                                                                                                                                                                                                                                                                   |
| client-identity-defaults | Displays default client-identities and their configuration                                                                                                                                                                                                                                                                              |
| configuration-revision   | Displays current configuration revision number                                                                                                                                                                                                                                                                                          |
| mac-user-import-status   | Displays status of file import initiated by a MAC-user                                                                                                                                                                                                                                                                                  |
| mac-vendor <OUI/MAC>     | Displays vendor name for a specified MAC address or OUI (Organizationally Unique Identifier) part of the MAC address <ul style="list-style-type: none"> <li>• &lt;OUI/MAC&gt; – Specify the MAC address or its OUI. The first six digits of the MAC address is the OUI. Use the AABBC or AA-BB-CC format to provide the OUI.</li> </ul> |
| noc diag                 | Displays NOC diagnostic details                                                                                                                                                                                                                                                                                                         |

|               |                               |
|---------------|-------------------------------|
| snmp session  | Displays SNMP session details |
| xpath-history | Displays XPath history        |

```
service show [command-history|crash-info|info|mem|process|reboot-history|
startup-log|ssh-authorized-keys|sysinfo|top|upgrade-history|watchdog] {on <DEVICE-NAME>}
```

|                  |                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show             | Displays running system statistics based on the parameters passed                                                                                                                                                                                                                                                                                                                 |
| command-history  | Displays command history (lists all commands executed)                                                                                                                                                                                                                                                                                                                            |
| crash-info       | Displays information about core, panic, and AP dump files                                                                                                                                                                                                                                                                                                                         |
| info             | Displays snapshot of available support information                                                                                                                                                                                                                                                                                                                                |
| mem              | Displays a system's current memory usage (displays the total memory and available memory)                                                                                                                                                                                                                                                                                         |
| process          | Displays active system process information (displays all processes currently running on the system)                                                                                                                                                                                                                                                                               |
| reboot-history   | Displays the device's reboot history                                                                                                                                                                                                                                                                                                                                              |
| startup-log      | Displays the device's startup log                                                                                                                                                                                                                                                                                                                                                 |
| sysinfo          | Displays system's memory usage information                                                                                                                                                                                                                                                                                                                                        |
| top              | Displays system resource information                                                                                                                                                                                                                                                                                                                                              |
| upgrade-history  | Displays the device's upgrade history (displays details, such as date, time, and status of the upgrade, old version, new version, etc.)                                                                                                                                                                                                                                           |
| watchdog         | Displays the device's watchdog status                                                                                                                                                                                                                                                                                                                                             |
| on <DEVICE-NAME> | The following keywords are common to all of the above: <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; - Optional. Displays information for a specified device. If no device is specified, the system displays information for logged device(s)</li> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
service show ip-access-list wlan <WLAN-NAME> status {detail} {on <DEVICE-OR-DOMAIN-NAME>}
```

|                     |                                                                                                                                                                                            |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show ip-access-list | Displays status of IP ACL to WLAN mappings on a specified device or all devices within a specified RF Domain. This command also displays if IP ACLs are properly applied in the dataplane. |
| wlan <WLAN-NAME>    | Specifies the WLAN, for which the IP ACL to WLAN mapping status is required <ul style="list-style-type: none"> <li>• &lt;WLAN-NAME&gt; - Specify the WLAN name.</li> </ul>                 |

|                            |                                                                                                                                                                                                                                                                                                                                          |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| status detail              | <p>Displays only failed IP ACL to WLAN mappings</p> <ul style="list-style-type: none"> <li>• details – Optional. Displays all (failed as well as successful) IP ACL to WLAN mapping status</li> </ul>                                                                                                                                    |
| on <DEVICE-OR-DOMAIN-NAME> | <p>Optional. Specifies the device name or the RF Domain name.</p> <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the device name or the RF Domain. When specified, the system displays IP ACL to WLAN mapping status on the specified device or all devices within the specified RF Domain.</li> </ul> |

```
service show dhcp-lease {<INTERFACE-NAME>/on/pppoe1/vlan <1-4094>/wwan1}
{(on <DEVICE-NAME>)}
```

|                  |                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show             | Displays running system statistics based on the parameters passed                                                                                                                                                                                                                                                                                                                                     |
| dhcp-lease       | Displays DHCP lease information received from the server                                                                                                                                                                                                                                                                                                                                              |
| <INTERFACE>      | <p>Optional. Displays DHCP lease information for a specified router interface</p> <ul style="list-style-type: none"> <li>• &lt;INTERFACE&gt; – Specify the router interface name.</li> </ul>                                                                                                                                                                                                          |
| on               | Optional. Displays DHCP lease information for a specified device                                                                                                                                                                                                                                                                                                                                      |
| pppoe1           | Optional. Displays DHCP lease information for a PPP over Ethernet interface                                                                                                                                                                                                                                                                                                                           |
| vlan <1-4094>    | <p>Optional. Displays DHCP lease information for a VLAN interface</p> <ul style="list-style-type: none"> <li>• &lt;1-4094&gt; – Specify a VLAN index from 1 - 4094.</li> </ul>                                                                                                                                                                                                                        |
| wwan1            | Optional. Displays DHCP lease information for a Wireless WAN interface                                                                                                                                                                                                                                                                                                                                |
| on <DEVICE-NAME> | <p>The following keywords are common to all of the above:</p> <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; – Optional. Displays DHCP lease information for a specified device. If no device is specified, the system displays information for the logged device.</li> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
service show diag [fds|pkts]
```

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show diag [fds pkts] | Displays diagnostic statistics, such as LED status, fan speed, sensor temperature, open file descriptors, looped packets, etc.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| fds                  | Displays the number of fds (file descriptors) opened by key processes, such as the CFGD. When executed, the command displays only the file name and FD.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| pkts                 | <p>Displays details of looped packets captured by the dataplane and pushed to a separate queue. These queued packets are written to a log file (named loop_pkt_info.log) available at the /var2/log/ directory. Use the <b>service &gt; start-shell</b> command and enter the path 'cat /var2/log/' to view if the loop_pkt_info.log file exists. However, looped packet logging has to be enabled in the profile/device context. For more information, see <a href="#">diag</a> on page 983 (profile config mode).</p> <p>The dataplane can log up to 16 looped packets at a time. Once the queue is full, no new loop packet is logged until the existing queue is cleared. To clear the logged looped packet queue execute the <b>service &gt; clear &gt; diag &gt; pkts</b> command.</p> <p>Following are the loop codes and the corresponding loop reasons:</p> <ul style="list-style-type: none"> <li>• (5) - "pkt looping in dataplane"</li> <li>• (51) - "loop in packet path"</li> <li>• (367) - "wispe encapsulation loop"</li> <li>• (432) - "mcx loop prevention"</li> <li>• (532) - "Port loop detected"</li> <li>• (536) - "packet loop detected by wireless bridge"</li> <li>• (41) - "IPv4 TTL exceeded"</li> <li>• (493) - "IPv6 TTL exceeded"</li> <li>• (540) - "mint TTL exceeded"</li> </ul> |

```
service show diag [led-status|psu|stats] {(on <DEVICE-NAME>)}
```

|                  |                                                                                                                                                                                                                                                                                                           |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show             | Displays running system statistics based on the parameters passed                                                                                                                                                                                                                                         |
| diag             | Displays diagnostic statistics, such as LED status, fan speed, and sensor temperature                                                                                                                                                                                                                     |
| led-status       | Displays LED state variables and the current state                                                                                                                                                                                                                                                        |
| psu              | Displays power supply information                                                                                                                                                                                                                                                                         |
| stats            | Displays fan speed and sensor temperature statistics                                                                                                                                                                                                                                                      |
| on <DEVICE-NAME> | <p>Optional. Displays diagnostic statistics for a specified device. If no device is specified, the system displays information for the logged device.</p> <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
service show guest-registration [export-status|import-status|restore-status]
```

|                    |                                                                                                                                                                                                                                                                                          |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show               | Displays running system statistics based on the parameters passed                                                                                                                                                                                                                        |
| guest-registration | <p>Displays status of the guest-registration database snapshot related processes (export, import, and restore)</p> <p><b>Note:</b> To export, import, or restore a guest-registration database, use the <b>service &gt; guest-registration &gt; [backup export import]</b> command.]</p> |
| export-status      | Displays the status of the latest export process initiated                                                                                                                                                                                                                               |

|               |                                                             |
|---------------|-------------------------------------------------------------|
| import-status | Displays the status of the latest import process initiated  |
| export-status | Displays the status of the latest restore process initiated |

```
service show fast-switching {on <DEVICE-NAME>}
```

|                  |                                                                                                                                                                                                                                            |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show             | Displays running system statistics based on the parameters passed                                                                                                                                                                          |
| fast-switching   | Displays fast switching state (enabled or disabled)                                                                                                                                                                                        |
| on <DEVICE-NAME> | Optional. Displays fast switching state for a specified device. If no device is specified, the system displays information for the logged device.<br><DEVICE-NAME> - Specify the name of the AP, wireless controller, or service platform. |

```
service show [fib|fib6] {table-id <0-255>}
```

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show             | Displays running system statistics based on the parameters passed                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| fib              | Displays entries in the FIB (Forwarding Information Base)                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| fib6             | Displays FIB IPv6 static routing entries<br>The WiNG software allows the IPv6 FIB to maintain only IPv6 static and interface routes. FIB is a collection of routing entries. A route entry consists of IPv6 network (which can also be a host) address, the prefix length for the network (for IPv6 routes this is between 0 - 128), and the next hop's (gateway) IPv6 address. Since a destination can be reached through multiple next hops, you can configure multiple routes to the same destination with multiple next hops. |
| table-id <0-255> | Optional. Displays FIB information maintained by the system based on the table ID<br>• <0-255> - Specify the table ID from 0 - 255.                                                                                                                                                                                                                                                                                                                                                                                               |

```
service show mint [adopted-devices {on <DEVICE-NAME>}|ports]
```

|                                  |                                                                                                                                                                                                                                                                                                             |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show                             | Displays running system statistics based on the parameters passed                                                                                                                                                                                                                                           |
| mint                             | Displays MiNT protocol details                                                                                                                                                                                                                                                                              |
| adopted-devices on <DEVICE-NAME> | Displays adopted devices status in dpd2<br>on <DEVICE-NAME> - Optional. Displays MiNT protocol details for a specified device. If no device is specified, the system displays information for the logged device.<br>• <DEVICE-NAME> - Specify the name of the AP, wireless controller, or service platform. |
| ports                            | Displays MiNT ports used by various services and features                                                                                                                                                                                                                                                   |

```
service show pm {history} {(on <DEVICE-NAME>)}
```

|                  |                                                                                                                                                                                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show             | Displays running system statistics based on the parameters passed                                                                                                                                                                              |
| pm               | Displays the PM (Process Monitor) controlled process details                                                                                                                                                                                   |
| history          | Optional. Displays process change history (the time at which the change was implemented, and the events that triggered the change)                                                                                                             |
| on <DEVICE-NAME> | Optional. Displays process change history for a specified device. If no device is specified, the system displays information for the logged device.<br>• <DEVICE-NAME> - Specify the name of the AP, wireless controller, or service platform. |

```
service show rf-domain-manager [diag|info] {<MAC/HOSTNAME>}
{(on <DEVICE-OR-DOMAIN-NAME>)}
```

|                            |                                                                                                                                                                                                                                                                                                                        |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show                       | Displays running system statistics based on the parameters passed                                                                                                                                                                                                                                                      |
| rf-domain-manager          | Displays RF Domain manager information                                                                                                                                                                                                                                                                                 |
| diag                       | Displays RF Domain manager related diagnostics statistics                                                                                                                                                                                                                                                              |
| info                       | Displays RF Domain manager related information                                                                                                                                                                                                                                                                         |
| <MAC/HOSTNAME>             | The following keyword is common to the 'diag' and 'info' parameters:<br>Optional. Specify the MAC address or hostname of the RF Domain manager.                                                                                                                                                                        |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is common to the 'diag' and 'info' parameters:<br>Optional. Displays diagnostics statistics on a specified device or domain <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; - Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> |

`service show sites`

|       |                                                                   |
|-------|-------------------------------------------------------------------|
| show  | Displays running system statistics based on the parameters passed |
| sites | Displays NOC sites related information                            |

`service show virtual-machine-history { (on <DEVICE-NAME> ) }`

|                              |                                                                                                                                                                                                                                                                         |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show virtual-machine-history | Displays virtual machine history based on the parameters passed<br>This command is applicable only to the NX 95XX and NX 96XX series service platforms. It is also available on the Privilege Executable Mode of these devices.                                         |
| on <DEVICE-NAME>             | Optional. Displays virtual machine history on a specified device. If no device is specified, the system displays information for the logged device. <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the service platform.</li> </ul> |

`service show wireless [aaa-stats|adaptivity-status|credential-cache|dns-cache|radar-status|vlan-usage] {on <DEVICE-NAME> }`

|                   |                                                                                                                                                                                                            |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show              | Displays running system statistics based on the parameters passed                                                                                                                                          |
| wireless          | Displays WLAN statistics (WLAN AAA policy, configuration parameters, VLAN assignment, etc.)                                                                                                                |
| aaa-stats         | Displays AAA policy statistics                                                                                                                                                                             |
| adaptivity-status | Displays the current list of channels (with interference levels exceeding the configured threshold resulting in adaptivity kicking in) and time when adaptivity kicked in on a device                      |
| credential-cache  | Displays clients cached credentials statistics (VLAN, keys, etc.)                                                                                                                                          |
| dns-cache         | Displays cache of resolved names of servers related to wireless networking                                                                                                                                 |
| radar-status      | Displays radar discovery status. This option displays following information: <ul style="list-style-type: none"> <li>• If a radar has been discovered by the AP</li> <li>• The time of discovery</li> </ul> |



|                  |                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vlan-usage       | Displays VLAN statistics across WLANs                                                                                                                                                                                                                                                                                                                                                        |
| on <DEVICE-NAME> | The following keywords are common to all of the above: <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; – Optional. Displays running system statistics on a specified device. If no device is specified, the system displays information for the logged device.</li> <li>&lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
service show wireless [config-internal|log-internal|neighbors]
```

|                 |                                                                                        |
|-----------------|----------------------------------------------------------------------------------------|
| show            | Displays running system statistics based on the parameters passed                      |
| wireless        | Displays WLAN statistics (WLAN AAA policy, configuration parameters, VLAN usage, etc.) |
| config-internal | Displays internal configuration parameters                                             |
| log-internal    | Displays recent internal wireless debug logs (info and above severity)                 |
| neighbors       | Displays neighboring device statistics for roaming and flow migration                  |

```
service show wireless [client|meshpoint neighbor] proc [info|stats] {<MAC>}
{(on <DEVICE-OR-DOMAIN-NAME>)}
```

|                            |                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show                       | Displays running system statistics based on the parameters passed                                                                                                                                                                                                                                                                                                                               |
| wireless                   | Displays WLAN statistics (WLAN AAA policy, configuration parameters, VLAN usage, etc.)                                                                                                                                                                                                                                                                                                          |
| client                     | Displays WLAN client statistics                                                                                                                                                                                                                                                                                                                                                                 |
| meshpoint neighbor         | Displays meshpoint related proc entries                                                                                                                                                                                                                                                                                                                                                         |
| proc                       | The following keyword is common to client and meshpoint neighbor parameters: <ul style="list-style-type: none"> <li>proc – Displays dataplane proc entries based on the parameter selected</li> </ul> <p><b>Note:</b> These proc entries provide statistics on each wireless client on the WLAN.</p> <p><b>Note:</b> For the meshpoint parameter, it displays proc entries about neighbors.</p> |
| info                       | This parameter is common to client and meshpoint neighbor parameters. Displays information for a specified device (wireless client or neighbor) or RF Domain.                                                                                                                                                                                                                                   |
| stats                      | This parameter is common to client and meshpoint neighbor parameters. Displays information for a specified device (wireless client or neighbor) or RF Domain.                                                                                                                                                                                                                                   |
| <MAC>                      | Displays information for a specified device (wireless client or neighbor) or RF Domain.                                                                                                                                                                                                                                                                                                         |
| on <DEVICE-OR-DOMAIN-NAME> | This parameter is common to client and meshpoint neighbor parameters. Displays information for a specified device (wireless client or neighbor) or RF Domain. <ul style="list-style-type: none"> <li>&lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul>                                                                |

```
service show wireless radio-internal [radio1|radio2] <LINE>
```

|          |                                                                                        |
|----------|----------------------------------------------------------------------------------------|
| show     | Displays running system statistics based on the parameters passed                      |
| wireless | Displays WLAN statistics (WLAN AAA policy, configuration parameters, VLAN usage, etc.) |

|                                |                                                                                                                                                                                                |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| radio-internal [radio1 radio2] | Displays radio internal debug logs. Select the radio from the following options: <ul style="list-style-type: none"> <li>radio1 – Selects radio 1</li> <li>radio2 – Selects radio 2.</li> </ul> |
| <LINE>                         | Specify the radio internal debug command to enable.                                                                                                                                            |

```
service show wireless reference [channels|frame|handshake|mcs-rates|reason-codes|
status-codes]
```

|              |                                                                                        |
|--------------|----------------------------------------------------------------------------------------|
| show         | Displays running system statistics based on the parameters passed                      |
| wireless     | Displays WLAN statistics (WLAN AAA policy, configuration parameters, VLAN usage, etc.) |
| reference    | Displays look up reference information related to standards, protocols, etc.           |
| channels     | Displays 802.11 channels information                                                   |
| frame        | Displays 802.11 frame structure                                                        |
| handshake    | Displays a flow diagram of 802.11 handshakes                                           |
| mcs-rates    | Displays MCS rate information                                                          |
| reason-codes | Displays 802.11 reason codes (for deauthentication, disassociation, etc.)              |
| status-codes | Displays 802.11 status codes (for association response)                                |

```
service show wireless stats-client diag {<MAC/HOSTNAME>}
{(on <DEVICE-OR-DOMAIN-NAME>) }
```

|                            |                                                                                                                                                                                                                                                       |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show                       | Displays running system statistics based on the parameters passed                                                                                                                                                                                     |
| wireless                   | Displays WLAN statistics (WLAN AAA policy, configuration parameters, VLAN usage etc.)                                                                                                                                                                 |
| stats-client               | Displays managed AP statistics                                                                                                                                                                                                                        |
| <MAC/HOSTNAME>             | Optional. Specify the MAC address or hostname of the AP.                                                                                                                                                                                              |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Displays statistics on a specified AP, or all APs on a specified domain. <ul style="list-style-type: none"> <li>&lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> |

```
service smart-rf clear-config {<MAC>|<DEVICE-NAME>|on <DOMAIN-NAME>}
```

|                  |                                                                                                                                                                                          |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| smart-rf         | Enables Smart RF management                                                                                                                                                              |
| clear-config     | Clears WLAN Smart RF configuration on a specified device or on all devices                                                                                                               |
| <MAC>            | Optional. Clears WLAN Smart RF configuration on a device identified by its MAC address. Specify the device's MAC address in the AA-BB-CC-DD-EE-FF format.                                |
| <DEVICE-NAME>    | Optional. Clears WLAN Smart RF configuration on a device identified by its hostname. Specify the device's hostname.                                                                      |
| on <DOMAIN-NAME> | Optional. Clears WLAN Smart RF configuration on all devices in a specified RF Domain <ul style="list-style-type: none"> <li>&lt;DOMAIN-NAME&gt; – Specify the RF Domain name.</li> </ul> |

```
service smart-rf [clear-history|clear-interfering-aps|save-config] {on <DOMAIN-NAME>}
```

|                       |                                                                                                                                                                                            |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| smart-rf              | Enables Smart RF management                                                                                                                                                                |
| clear-history         | Clears WLAN Smart RF history on all devices                                                                                                                                                |
| clear-interfering-aps | Clears Smart-RF interfering APs                                                                                                                                                            |
| save-config           | Saves the Smart RF configuration on all devices, and also saves the history on the RF Domain Manager                                                                                       |
| on <DOMAIN-NAME>      | Optional. Clears WLAN Smart RF configuration on all devices in a specified RF Domain <ul style="list-style-type: none"> <li>• &lt;DOMAIN-NAME&gt; – Specify the RF Domain name.</li> </ul> |

`service snmp sysoid wing5`

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| service snmp sysoid wing5 | <p>Configures a new sysObjectID (sysoid), in the MIB, for devices running WiNG 5.X devices</p> <p>When configured, the SNMP manager returns sysoid for WiNG 5.X OS. Hardwares running the WiNG 4.X and WiNG 5.X images have different sysoids. For example, the sysoid for a RFS4010 using the WiNG 4.X image differs from another RFS4010 running the WiNG 5.X image.</p> <p>This command is applicable only to RFS4010 platform, since it has the same sysoid supported in WiNG 4.X and WiNG 5.X.</p> <p>The WiNG 4.X sysoids are:</p> <ul style="list-style-type: none"> <li>• RFS4010 - 1.3.6.1.4.1.388.18</li> </ul> <p>The WiNG 5.X sysoids are:</p> <ul style="list-style-type: none"> <li>• RFS4010 - 1.3.6.1.4.1.388.50.11.35</li> </ul> |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

`service ssm dump-core-snapshot`

|                                |                                              |
|--------------------------------|----------------------------------------------|
| service ssm dump-core-snapshot | Triggers a debug core dump of the SSM module |
|--------------------------------|----------------------------------------------|

`service syslog test {level [<0-7>|alerts|critical|debugging|emergencies|errors|informational|notifications|warnings]} {(on <DEVICE-NAME>)}`

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| syslog test      | <p>Sends a test message to the syslog server to confirm server availability</p> <p>Optional. Sets the logging level. In case syslog server is unreachable, an event is logged based on the logging level defined. This is an optional parameter, and the system configures default settings, if no logging severity level is specified.</p> <ul style="list-style-type: none"> <li>• &lt;0-7&gt; – Optional. Specify the logging severity level from 0-7. The various levels and their implications are as follows: <ul style="list-style-type: none"> <li>• alerts – Optional. Immediate action needed (severity=1)</li> <li>• critical – Optional. Critical conditions (severity=2)</li> <li>• debugging – Optional. Debugging messages (severity=7)</li> <li>• emergencies – Optional. System is unusable (severity=0)</li> <li>• errors – Optional. Error conditions (severity=3)</li> <li>• informational – Optional. Informational messages (severity=6)</li> <li>• notifications – Optional. Normal but significant conditions (severity=5)</li> <li>• warnings – Optional. Warning conditions (severity=4). This is the default setting.</li> </ul> </li> </ul> |
| on <DEVICE-NAME> | <p>Optional. Executes the command on a specified device</p> <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

```
service ssm trace pattern <WORD> {on <DOMAIN-NAME>}
```

|                  |                                                                                                                                                                                                                      |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ssm trace        | Displays the SSM module trace based on parameters passed                                                                                                                                                             |
| pattern <WORD>   | <p>Configures the pattern to match</p> <p>&lt;WORD&gt; – Specify the pattern to match.</p>                                                                                                                           |
| on <DEVICE-NAME> | <p>Optional. Displays the SSM module trace on a specified device</p> <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
service wireless client beacon-request <MAC> mode [active|passive|table]
ssid [<SSID>|any] channel-report [<CHANNEL-LIST>|none] {on <DEVICE-NAME>}
```

|                                 |                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless client beacon-requests | Sends beacon measurement requests to a wireless client                                                                                                                                                                                                                                                                                |
| <MAC>                           | Specify the wireless client's MAC address.                                                                                                                                                                                                                                                                                            |
| mode [active passive table]     | <p>Specifies the beacon measurement mode. The following modes are available:</p> <ul style="list-style-type: none"> <li>• Active – Requests beacon measurements in the active mode</li> <li>• Passive – Requests beacon measurements in the passive mode</li> <li>• Table – Requests beacon measurements in the table mode</li> </ul> |
| ssid [<SSID> any]               | <p>Specifies if the measurements have to be made for a specified SSID or for any SSID</p> <ul style="list-style-type: none"> <li>• &lt;SSID&gt; – Requests beacon measurement for a specified SSID</li> <li>• any – Requests beacon measurement for any SSID</li> </ul>                                                               |

|                                       |                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| channel-report [<CHANNEL-LIST>  none] | Configures channel report in the request. The request can include a list of channels or can apply to all channels. <ul style="list-style-type: none"> <li>• &lt;CHANNEL-LIST&gt; - Request includes a list of channels. The client has to send beacon measurements only for those channels included in the request.</li> <li>• none - Request applies to all channels</li> </ul> |
| on <DEVICE-NAME>                      | Optional. Sends requests on a specified device <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul>                                                                                                                                                                                   |

```
service wireless client quiet-element [start|stop]
```

|                                        |                                                                                                                                                            |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless client trigger-bss-transition | Enables the quiet-element information in beacons sent to wireless clients                                                                                  |
| start                                  | Enables the quiet-element information in beacons sent to wireless clients. This is the start of the time period when wireless clients are to remain quiet. |
| stop                                   | Disables the quiet-element information in beacons sent to wireless clients. Once disabled, this information is no longer included in beacons.              |

```
service wireless client trigger-bss-transition mac <MAC> {timeout <0-65535>
{url <URL>} {on <DEVICE-OR-DOMAIN-NAME>}}
```

|                                        |                                                                                                                                                                                                                                                                                        |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless client trigger-bss-transition | Sends a 80211v-Wireless Network Management BSS transition request to a client                                                                                                                                                                                                          |
| <MAC>                                  | Specifies the wireless client's MAC address                                                                                                                                                                                                                                            |
| timeout <0-65535>                      | Specifies the time remaining, for this client, before BSS transition is initiated. In other words on completion of the specified time period, BSS transition is triggered. <ul style="list-style-type: none"> <li>• &lt;0-65535&gt; - Specify a time from 0 -65535 seconds.</li> </ul> |
| url <URL>                              | Specifies session termination URL                                                                                                                                                                                                                                                      |
| on <DEVICE-OR-DOMAIN-NAME>             | Optional. Sends request on a specified device <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR_DOMAIN-NAME&gt; - Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul>                                                                     |

```
service wireless client trigger-wnm mac <MAC> type [deauth-imminent|
subscription-remediation] {uri <WORD>}
```

|                                                  |                                                                                                                                                                                                                                         |
|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless client trigger-wnm                      | Sends a WNM notification (action frame) to a wireless client                                                                                                                                                                            |
| mac <MAC>                                        | Specifies the wireless client's MAC address                                                                                                                                                                                             |
| type [deauth-imminent  subscription-remediation] | Configures the WNM notification type <ul style="list-style-type: none"> <li>• deauth-imminent - Sends a de-authentication imminent frame</li> <li>• subscription-remediation - Sends a subscription remediation needed frame</li> </ul> |
| uri <WORD>                                       | Optional. Specifies the unique resource identifier (URI)                                                                                                                                                                                |

```
service wireless dump-core-snapshot
```

|                             |                                                   |
|-----------------------------|---------------------------------------------------|
| wireless dump-core-snapshot | Triggers a debug core dump of the wireless module |
|-----------------------------|---------------------------------------------------|

```
service wireless meshpoint zl <MESHPOINT-NAME> [on <DEVICE-NAME>] {<ARGS>/
timeout <1-65535>}
```

|                               |                                                                                                                                                                                                                                                                                     |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| service wireless meshpoint zl | Triggers a zonal level debug of a specified meshpoint's modules                                                                                                                                                                                                                     |
| <MESHPOINT-NAME>              | Specify the meshpoint name                                                                                                                                                                                                                                                          |
| on <DEVICE-NAME>              | Triggers zonal level debug of a specified meshpoint's modules on a specified device <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; - Specify the name of the device (AP, wireless controller, or service platform)</li> </ul>                                           |
| <ARGS>                        | Optional. Specifies the zonal arguments. These zonal arguments represent the meshpoint modules identified by the zonal and subzonal arguments passed here. Also specify the debug level from 0 -7. Please see the Examples section, at the end of this topic, for more information. |
| timeout <1-65535>             | Optional. Specifies a timeout value from 1 - 65535 seconds. When specified, meshpoint logs are debugged for the time specified here.                                                                                                                                                |

```
service wireless qos delete-tspec <MAC> tid <0-7>
```

|                           |                                                                                                                                 |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| wireless qos delete-tspec | Sends a delete TSPEC request to a wireless client                                                                               |
| <MAC>                     | Specify the MAC address of the wireless client.                                                                                 |
| tid <0-7>                 | Deletes the TID (Traffic Identifier) <ul style="list-style-type: none"> <li>&lt;0-7&gt; - Select the TID from 0 - 7.</li> </ul> |

```
service wireless trace pattern <WORD> {on <DEVICE-NAME>}
```

|                  |                                                                                                                                                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless trace   | Displays the wireless module trace based on parameters passed                                                                                                                                                    |
| pattern <WORD>   | Configures the pattern to match <ul style="list-style-type: none"> <li>&lt;WORD&gt; - Specify the pattern to match.</li> </ul>                                                                                   |
| on <DEVICE-NAME> | Optional. Displays the wireless module trace on a specified device <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
service wireless unsanctioned ap air-terminate <MAC> {on <DOMAIN-NAME>}
```

|                                        |                                                                                                                                                                  |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless unsanctioned ap air-terminate | Enables unsanctioned access points termination                                                                                                                   |
| <MAC>                                  | Configures the unsanctioned access points' BSSID (MAC address)                                                                                                   |
| on <DOMAIN-NAME>                       | Optional. Specifies the RD Domain of the access point <ul style="list-style-type: none"> <li>&lt;DOMAIN-NAME&gt; - Specify the name of the RF Domain.</li> </ul> |

```
service wireless wips clear-client-blacklist [all|mac <MAC>]
```



|                                        |                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless wips                          | Enables management of WIPS parameters                                                                                                                                                                                                                                                                                                            |
| clear-client-blacklist [all mac <MAC>] | Removes a specified client or all clients from the blacklist <ul style="list-style-type: none"> <li>all - Removes all clients from the blacklist</li> <li>mac &lt;MAC&gt; - Removes a specified client from the blacklist <ul style="list-style-type: none"> <li>&lt;MAC&gt; - Specify the wireless client's MAC address.</li> </ul> </li> </ul> |

```
service wireless wips clear-event-history {on <DEVICE-OR-DOMAIN-NAME>}
```

|                            |                                                                                                                                                                                                                            |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless wips              | Enables management of WIPS parameters                                                                                                                                                                                      |
| clear-event-history        | Clears event history                                                                                                                                                                                                       |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Clears event history on a device or RF Domain <ul style="list-style-type: none"> <li>&lt;DEVICE-OR-DOMAIN-NAME&gt; - Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> |

## Syntax (Privilege Exec Mode)

### Service Commands - Intro



#### Note

The "service" command of the Priv Exec Mode is the same as the service command in the User Exec Mode. There are a few modifications that have been documented in this section. For the syntax and parameters of the other commands refer to the [Syntax \(User Exec Mode\)](#) and [Parameters \(User Exec Mode\)](#) sections of this chapter.

```
service [block-adopter-config-updates|clear|cli-tables-skin|cluster|copy|
database|delete|delete-offline-aps|force-send-config|force-update-vm-stats|
guest-registration|load-balancing|locator|mint|pktcap|pm|radio|radius|
request-full-config-from-adopter|restore|set|show|signal|smart-rf|snmp|ssm|
start-shell|syslog|trace|wireless]
service clear crash-info {on <DEVICE-NAME>}
service copy [stats-report|tech-support]
service copy stats-report [global|rf-domain <DOMAIN-NAME>] (<FILE>|<URL>)
service copy tech-support [<FILE>|<URL>]
service database [authentication|compact|drop|maintenance-mode|primary-stepdown|
remove-all-files|replica-set|server|start-shell]
service database authentication [create-user|delete-user]
service database authentication create-user username <USER-NAME> password <PASSWORD>
service database authentication delete-user username <USER-NAME>
service database compact [all|captive-portal|nsight]
service database [maintenance-mode|primary-stepdown|remove-all-files|start-shell]
service database replica-set [add|delete]
service database replica-set add member [<IP>|<FQDN>] [arbiter|priority <0-255>]
service database replica-set delete member [<IP>|<FQDN>]
service database server [restart|start|stop]
service delete sessions <SESSION-COOKIES>
service mint [clear|debug-log|expire|flood]
service mint [clear [lsp-db|mlcp]|debug-log [flash-and-syslog|flash-only]|
expire [lsp|spf]|flood [csnp|lsp]]
service pktcap on [bridge|deny|drop|ext-vlan|interface|radio|rim|router|vpn|wireless]
service pktcap on [bridge|deny|drop|ext-vlan|rim|router|vpn|wireless]
{(acl-name <ACL>,count <1-100000>,direction [any|inbound|outbound],filter <LINE>,
hex,rate <1-100>,snap <1-2048>,tcpdump,verbose,write [file|url|
tzsp [<IP/TZSP-HOSTNAME>]])}
service pktcap on interface [<INTERFACE-NAME>|ge <1-4>|me1|port-channel <1-2>|
pppoe1|vlan <1-4094>|wwan1] {(acl-name <ACL>,count <1-100000>,
```

```

direction [any|inbound|outbound],filter <LINE>,hex,rate <1-100>,snap <1-2048>,
tcpdump,verbose,write [file|url|tzsp [<IP/TZSP-HOSTNAME>]]}
service pktcap on radio [<1-1024>|all] {(acl-name <ACL>,count <1-1000000>,
direction [any|inbound|outbound],filter <LINE>,hex,promiscuous,rate <1-100>,
snap <1-2048>,tcpdump,verbose,write [file|url|tzsp [<IP/TZSP-HOSTNAME>]])}
service pm stop {on <DEVICE-NAME>}
service restore analytics-support [<FILE>|<URL>]
service show last-passwd
service signal [abort <PROCESS-NAME>|kill <PROCESS-NAME>]
service start-shell
service trace <PROCESS-NAME> {summary}

```

## Parameters (Privilege Exec Mode)

### Service Commands - Intro

```
service copy tech-support <FILE> <URL>
```

|                   |                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| copy tech-support | Copies extensive system information used for troubleshooting                                                                                                                                                                                                                                                                                                                             |
| <FILE>            | Specify the location of the file to be copied, using the following format: <ul style="list-style-type: none"> <li>usbX:/path/file</li> </ul>                                                                                                                                                                                                                                             |
| <URL>             | Specify the location URL of the file to be copied. Both IPv4 and IPv6 address formats are supported. <ul style="list-style-type: none"> <li>tftp://&lt;hostname IPv4/IPv6&gt;[:port]/path/file</li> <li>ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IPv4/IPv6&gt;[:port]/path/file</li> <li>sftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IPv4/IPv6&gt;[:port]/path/file</li> </ul> |

```
service copy stats-report [global|rf-domain <DOMAIN-NAME>] (<FILE>|<URL>)
```

|                                  |                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| copy stats-report                | Copies extensive statistical data useful for troubleshooting                                                                                                                                                                                                                                                                                                                             |
| [global rf-domain <DOMAIN-NAME>] | Identifies the RF Domain to copy statistical data <ul style="list-style-type: none"> <li>global - Copies extensive statistical data of all configured RF Domains</li> <li>rf-domain &lt;DOMAIN-NAME&gt; - Copies extensive statistical data of a specified RF Domain. Specify the domain name.</li> </ul>                                                                                |
| <FILE>                           | Specify the location to copy file using the following format: <ul style="list-style-type: none"> <li>usbX:/path/file</li> </ul>                                                                                                                                                                                                                                                          |
| <URL>                            | Specify the location URL of the file to be copied. Both IPv4 and IPv6 address formats are supported. <ul style="list-style-type: none"> <li>tftp://&lt;hostname IPv4/IPv6&gt;[:port]/path/file</li> <li>ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IPv4/IPv6&gt;[:port]/path/file</li> <li>sftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IPv4/IPv6&gt;[:port]/path/file</li> </ul> |

```
service clear crash-info {on <DEVICE-NAME>}
```

|                  |                                                                                                                                                                                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| clear crash-info | Clears all crash files                                                                                                                                                                                                                           |
| on <DEVICE-NAME> | Optional. Clears crash files on a specified device. These crash files are core, panic, and AP dump <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
service database authentication create-user username <USER-NAME> password <PASSWORD>
```



|                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| database                                                                  | <p>Performs database related actions</p> <p><b>Note:</b> This command is supported only on the NX 95XX, NX 96XX, and VX 9000 platforms.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| authentication create-user<br>username <USER-NAME><br>password <PASSWORD> | <p>Creates users having access rights to the database. Execute this command on the database host. However, before creating users, on the database, generate the database keyfile. For more information on generating the keyfile, see <a href="#">database</a> (user exec mode).</p> <ul style="list-style-type: none"> <li>username &lt;USER-NAME&gt; - Configures database username <ul style="list-style-type: none"> <li>password &lt;PASSWORD&gt; - Configures a password for the username specified above</li> </ul> </li> </ul> <p>In the database-policy ensure that authentication is enabled and username and password is configured. The database-client-policy also should have the same username and password configured. For more information on database-policy and database-client-policy, see <a href="#">database-policy</a> and <a href="#">database-client-policy</a> (global config mode).</p> |

```
service database authentication delete-user username <USER-NAME>
```

|                                                          |                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| database                                                 | <p>Performs database related actions</p> <p><b>Note:</b> This command is supported only on the NX 95XX, NX 96XX, and VX 9000 platforms.</p>                                                                                                                                                                                                             |
| database authentication delete-user username <USER-NAME> | <p>Deletes the username requires to access rights the captive-portal/NSight database</p> <ul style="list-style-type: none"> <li>username &lt;USER-NAME&gt; - Deletes the username identified by the &lt;USER-NAME&gt; keyword</li> </ul> <p>Once deleted, the database cannot be accessed using the specified combination of username and password.</p> |

```
service database compact [all|captive-portal|nsight]
```

|                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| database                              | <p>Performs database related actions</p> <p>This command is supported only on the NX 95XX, NX 96XX, and VX 9000 platforms.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| compact [all  captive-portal  nsight] | <p>Compacts collections within the database. Each database (captive-portal and NSight) contains one or more collection, where each collection is a set of records. Use this command to make a single compact set of all collections within a database.</p> <ul style="list-style-type: none"> <li>all - Compacts collections within all databases (captive-portal and NSight) being maintained</li> <li>captive-portal - Compacts all collections within the captive portal database only</li> <li>nsight - Compacts all collections within the NSight database only</li> </ul> |

```
service database [maintenance-mode|primary-stepdown|remove-all-files|start-shell]
```



|                  |                                                                                                                                                                                                                                                                         |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| database         | Performs database related actions<br><br><b>Note:</b> This command is supported only on the NX 95XX, NX 96XX, and VX 9000 platforms.                                                                                                                                    |
| maintenance-mode | Places the database server in the maintenance mode                                                                                                                                                                                                                      |
| primary-stepdown | Requests the primary replica-set to step down. For more information on replica-sets and its creation, see <a href="#">database-policy</a> (global config mode).                                                                                                         |
| remove-all-files | Removes all database-server related files (captive-portal and NSight). Use in a scenario where complete removal of all database related files is necessary, such as when downgrading to 5.8.1 or 5.8.0 version. Extreme caution is recommended when using this command. |
| start-shell      | Starts the database shell                                                                                                                                                                                                                                               |

```
service database replica-set add member [<IP>|<FQDN>] [arbiter|priority <0-255>]
```

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| database    | Performs database related actions<br><br><b>Note:</b> This command is supported only on the NX 95XX, NX 96XX, and VX 9000 platforms.                                                                                                                                                                                                                                                                                                                                                                                   |
| replica-set | Adds members to the database replica set. A replica set is a group of devices running the database instances that maintain the same data set. Replica sets provide redundancy and high availability, and are the basis for all production deployments. The replica set can contain a maximum of fifty (50) members, with each member (with the exception of the arbiter) hosting an instance of the database. For more information on creating replica sets, see <a href="#">database-policy</a> (global config mode). |

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| add member [<IP> <FQDN>]    | <p>Adds members to the database replica set</p> <ul style="list-style-type: none"> <li>• &lt;IP&gt; – Identifies the member by its IP address. Specify the member’s IP address.</li> <li>• &lt;FQDN&gt; – Identifies the member by its FQDN (Fully Qualified Domain Name). Specify the member’s FQDN address.</li> </ul> <p><b>Note:</b> Ensure that the identified members have the database instance running prior to being added to the replica set.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| [arbiter] priority <0-255>] | <p>After identifying the new member, optionally specify if the member is the arbiter or not. If not the arbiter, specify the member’s priority value.</p> <ul style="list-style-type: none"> <li>• arbiter – Identifies the new member as the arbiter. The arbiter does not maintain a data set and is added to the replica set to facilitate the election of the fall-back primary member. It provides that one extra vote required in the election of the primary member.</li> <li>• priority &lt;0-255&gt; – Identifies the new member as not being the arbiter and configures its priority value. <ul style="list-style-type: none"> <li>• &lt;0-255&gt; – Specify the priority value from 0 - 255. Not applicable for the arbiter.</li> </ul> </li> </ul> <p>The priority value determines the member’s position within the replica set as primary or secondary. It also helps in electing the fall-back primary member in the eventuality of the current primary member being unreachable. All identified members should have the database instances running prior to being added to the replica set.</p> |

`service database replica-set delete member [<IP>|<FQDN>]`

|                             |                                                                                                                                                                                                                                                                                                         |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| database                    | <p>Performs database related actions</p> <p><b>Note:</b> This command is supported only on the NX 95XX, NX 96XX, and VX 9000 platforms.</p>                                                                                                                                                             |
| replica-set                 | <p>Allows deletion of members in a database replica set. For each database a single three-member replica-set can be created and maintained. For more information on creating replica sets, see <a href="#">database-policy</a> (global config mode) .</p>                                               |
| delete member [<IP> <FQDN>] | <p>Deletes members from an existing database replica set</p> <ul style="list-style-type: none"> <li>• &lt;IP&gt; – Identifies the member by its IP address. Specify the member’s IP address.</li> <li>• &lt;FQDN&gt; – Identifies the member by its FQDN. Specify the member’s FQDN address.</li> </ul> |

|                             |                                                                                                                                                                                                                         |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| database                    | <p>Performs database related actions</p> <p><b>Note:</b> This command is supported only on the NX 95XX, NX 96XX, and VX 9000 platforms.</p>                                                                             |
| server [restart start stop] | <p>Performs the following actions on the database server:</p> <ul style="list-style-type: none"> <li>• restart – Restarts the server</li> <li>• start – Starts the server</li> <li>• stop – Stops the server</li> </ul> |

`service delete sessions <SESSION-COOKIES>`

```
delete sessions <SESSION-COOKIES> Deletes session cookies
 • <SESSION-COOKIES> - Provide a list of cookies to delete.
```

```
service mint [clear [lsp-db|mlcp]|debug-log [flash-and-syslog|flash-only]|
expire [lsp|spf]|flood [csnp|lsp]]
```

|                                         |                                                                                                                                                                                                                       |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mint                                    | Enables MiNT protocol management (clears LSP database, enables debug logging, enables running silence etc.)                                                                                                           |
| clear [lsp-db mlcp]                     | Clears LSP database and MLCP (MiNT Link Control Protocol) links <ul style="list-style-type: none"> <li>lsp-db - Clears MiNT LSP (Label Switched Path) database</li> <li>mlcp - Clears MLCP links</li> </ul>           |
| debug-log [flash-and-syslog flash-only] | Enables debug message logging <ul style="list-style-type: none"> <li>flash-and-syslog - Logs debug messages to the flash and syslog files</li> <li>flash-only - Logs debug messages to the flash file only</li> </ul> |
| expire [lsp spf]                        | Forces expiration of LSP and recalculation of SPF (Shortest Path First ) <ul style="list-style-type: none"> <li>lsp - Forces expiration of LSP</li> <li>spf - Forces recalculation of SPF</li> </ul>                  |
| flood [csnp lsp]                        | Floods control packets <ul style="list-style-type: none"> <li>csnp - Floods our CSNP (Complete Sequence Number Packets)</li> <li>lsp - Floods our LSP</li> </ul>                                                      |

```
service pm stop {on <DEVICE-NAME>}
```

|                  |                                                                                                                                                                                            |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| pm               | Stops the PM                                                                                                                                                                               |
| stops            | Stops the PM from monitoring all daemons                                                                                                                                                   |
| on <DEVICE-NAME> | Optional. Stops the PM on a specified device <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
service pktcap on [bridge|deny|drop|ext-vlan|rim|router|vpn|wireless]
{(acl-name <ACL>,count <1-1000000>,direction [any|inbound|outbound],filter,hex,rate
<1-100>,
snap <1-2048>,tcpdump,verbose,write [file/url|tzsp <IP/TZSP-HOSTNAME>])}
```

|           |                                                                                                                                                   |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| pktcap on | Captures data packets crossing at a specified location <ul style="list-style-type: none"> <li>on - Defines the packet capture location</li> </ul> |
| bridge    | Captures packets transiting through the Ethernet bridge                                                                                           |
| deny      | Captures packets denied by an ACL                                                                                                                 |
| drop      | Captures packets at the drop locations                                                                                                            |
| ext-vlan  | Captures packets forwarded to or from an extended VLAN                                                                                            |
| rim       | Captures packets at the RIM (Radio Interface Module)                                                                                              |
| router    | Captures packets transiting through an IP router                                                                                                  |
| vpn       | Captures packets forwarded to or from a VPN link                                                                                                  |
| wireless  | Captures packets forwarded to or from a wireless device                                                                                           |

|                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| acl-name <ACL>                                                                                                                                               | Optional. Specify the ACL that matches the ACL name for the 'deny' location                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| count <1-1000000>                                                                                                                                            | Optional. Limits the captured packet count. Specify a value from 1 -1000000.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| direction [any inbound outbound]                                                                                                                             | Optional. Changes the packet direction with respect to a device. The direction can be set as any, inbound, or outbound.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| filter [<LINE> arp capwap  cdp  dot11 dropreason  dst ether  host icmp  igmp ip ipv6 l2 l3 l4 lldp mint net not port  priority  radi src tcp udp  vlan wlan] | Optional. Filters packets based on the option selected (must be used as a last option). The filter options are: <ul style="list-style-type: none"> <li>• &lt;LINE&gt; – Defines user defined packet capture filter</li> <li>• arp – Matches ARP packets</li> <li>• capwap – Matches CAPWAP packets</li> <li>• cdp – Matches CDP packets</li> <li>• dot11 – Matches 802.11 packets</li> <li>• dropreason – Matches packet drop reason</li> <li>• dst – Matches IP destination</li> <li>• ether – Matches Ethernet packets</li> <li>• failed – Matches failed 802.11 transmitted frames</li> <li>• host – Matches host destination</li> <li>• icmp – Matches ICMP packets</li> <li>• icmp6 – Matches ICMPv6 frames</li> <li>• ip – Matches IPV4 packets</li> <li>• ipv6 – Matches IPV6 packets</li> <li>• l2 – Matches L2 header</li> <li>• l3 – Matches L3 header</li> <li>• l4 – Matches L4 header</li> <li>• mint – Matches MiNT packets</li> <li>• lldp – Matches LLDP packets</li> <li>• net – Matches IP in subnet</li> <li>• not – Filters out any packet that matches the filter criteria (For example, if not TCP is used, all tcp packets are filtered out)</li> <li>• port – Matches TCP or UDP port</li> <li>• priority – Matches packet priority</li> <li>• radio – Matches radio</li> <li>• rssi – Matches Received Signal Strength Indication (RSSI) of received radio signals</li> <li>• src – Matches IP source</li> <li>• stp – Matches STP packets</li> <li>• tcp – Matches TCP packets</li> <li>• tcp6 – Matches TCP over IPv6 packets</li> <li>• udp – Matches UDP packets</li> <li>• udp6 – Matches UDP over IPv6 packets</li> <li>• vlan – Matches VLAN</li> <li>• wlan – Matches WLAN</li> </ul> |
| hex                                                                                                                                                          | Optional. Provides binary output of the captured packets                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| rate <1-100>                                                                                                                                                 | Optional. Specifies the packet capture rate <ul style="list-style-type: none"> <li>• &lt;1-100&gt; – Specify a value from 1 - 100 seconds.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| snap <1-2048>                                                                                                                                                | Optional. Captures the data length <ul style="list-style-type: none"> <li>• &lt;1-2048&gt; – Specify a value from 1 - 2048 characters.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| tcpdump | Optional. Decodes tcpdump. The tcpdump analyzes network behavior, performance, and infrastructure. It also analyzes applications that generate or receive traffic.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| verbose | Optional. Displays full packet body                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| write   | <p>Captures packets to a specified file. Provide the file name and location in the following format:</p> <ul style="list-style-type: none"> <li>flash:/path/file</li> <li>usbX:/path/file</li> </ul> <p>URL – Specify the location URL to capture file. Both IPv4 and IPv6 address formats are supported.</p> <ul style="list-style-type: none"> <li>nvrn:startup-config</li> <li>tftp://&lt;hostname IP&gt;[:port]/path/file</li> <li>ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IP&gt;[:port]/path/file</li> <li>sftp://&lt;user&gt;@&lt;hostname IP&gt;[:port]/path/file</li> <li>tzsp – TZSP (Tazman Sniffer Protocol) host. Specify the TZSP host's IP address or hostname.</li> </ul> |

```
service pktcap on radio [<1-1024>|all] {(acl-name <ACL>,count <1-1000000>,
direction [any|inbound|outbound],filter <LINE>,hex,promiscuous,rate <1-100>,
snap <1-2048>,tcpdump,verbose,write [file|url|tzsp <IP/TZSP-HOSTNAME>])}
```

|                                  |                                                                                                                                                                                                                                           |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| pktcap on radio                  | Captures data packets on a radio (802.11)                                                                                                                                                                                                 |
| <1-1024>                         | <p>Captures data packets on a specified radio</p> <ul style="list-style-type: none"> <li>&lt;1-1024&gt; – specify the radio index from 1 - 1024.</li> </ul>                                                                               |
| all                              | Captures data packets on all radios                                                                                                                                                                                                       |
| acl-name <ACL>                   | Optional. Specify the ACL that matches the ACL name for the 'deny' location                                                                                                                                                               |
| count <1-1000000>                | <p>Optional. Sets a specified number of packets to capture</p> <ul style="list-style-type: none"> <li>&lt;1-1000000&gt; – Specify a value from 1 - 1000000.</li> </ul>                                                                    |
| direction [any inbound outbound] | Optional. Changes the packet direction with respect to a device. The direction can be set as <b>any</b> , <b>inbound</b> , or <b>outbound</b> .                                                                                           |
| filter <LINE>                    | <p>Optional. Filters packets based on the option selected (must be used as a last option)</p> <ul style="list-style-type: none"> <li>&lt;LINE&gt; – Define a packet capture filter or select any one of the available options.</li> </ul> |
| hex                              | Optional. Provides binary output of the captured packets                                                                                                                                                                                  |
| rate <1-100>                     | <p>Optional. Specifies the packet capture rate</p> <ul style="list-style-type: none"> <li>&lt;1-100&gt; – Specify a value from 1 - 100 seconds.</li> </ul>                                                                                |
| snap <1-2048>                    | <p>Optional. Captures the data length</p> <ul style="list-style-type: none"> <li>&lt;1-2048&gt; – Specify a value from 1 - 2048 characters.</li> </ul>                                                                                    |
| tcpdump                          | Optional. Decodes the TCP dump                                                                                                                                                                                                            |

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| verbose | Optional. Displays full packet body                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| write   | <p>Captures packets to a specified file. Provide the file name and location in the following format:</p> <ul style="list-style-type: none"> <li>flash:/path/file</li> <li>usbX:/path/file</li> </ul> <p>URL – Specify the location URL to capture file. Both IPv4 and IPv6 address formats are supported.</p> <ul style="list-style-type: none"> <li>nvrn:startup-config</li> <li>tftp://&lt;hostname IP&gt;[:port]/path/file</li> <li>ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IP&gt;[:port]/path/file</li> <li>sftp://&lt;user&gt;@&lt;hostname IP&gt;[:port]/path/file</li> <li>tzsp – TZSP (Tazman Sniffer Protocol) host. Specify the TZSP host's IP address or hostname.</li> </ul> |

```
service pktcap on interface [<INTERFACE>|ge <1-4>|me|port-channel <1-2>|vlan
<1-4094>] {(acl-name <ACL>,count <1-1000000>,direction [any|inbound|outbound],
filter <LINE>,hex,rate <1-100>,snap <1-2048>,tcpdump,verbose,
write [file/url/tzsp <IP/TZSP-HOSTNAME>])}
```

|                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| pktcap on                                                                | <p>Captures data packets at a specified interface</p> <ul style="list-style-type: none"> <li>on – Specify the capture location.</li> </ul>                                                                                                                                                                                                                                                                                                                |
| interface [<INTERFACE>  ge <1-4>  me  port-channel <1-2>  vlan <1-4094>] | <p>Captures packets at a specified interface. The options are:</p> <ul style="list-style-type: none"> <li>&lt;INTERFACE&gt; – Specify the interface name.</li> <li>ge &lt;1-4&gt; – Selects a GigabitEthernet interface index from 1 - 4</li> <li>me1 – Selects the FastEthernet interface</li> <li>port-channel &lt;1-2&gt; – Selects a port-channel interface index from 1- 2</li> <li>vlan &lt;1-4094&gt; – Selects a VLAN ID from 1 - 4094</li> </ul> |
| acl-name <ACL>                                                           | Optional. Specify the ACL that matches the ACL name for the 'deny' location                                                                                                                                                                                                                                                                                                                                                                               |
| count <1-1000000>                                                        | <p>Optional. Sets a specified number of packets to capture</p> <ul style="list-style-type: none"> <li>&lt;1-1000000&gt; – Specify a value from 1 - 1000000.</li> </ul>                                                                                                                                                                                                                                                                                    |
| direction [any inbound outbound]                                         | Optional. Changes the packet direction with respect to a device. The direction can be set as any, inbound, or outbound.                                                                                                                                                                                                                                                                                                                                   |
| filter <LINE>                                                            | <p>Optional. Filters packets based on the option selected (must be used as a last option)</p> <ul style="list-style-type: none"> <li>&lt;LINE&gt; – Define a packet capture filter or select any one of the available options.</li> </ul>                                                                                                                                                                                                                 |
| hex                                                                      | Optional. Provides binary output of the captured packets                                                                                                                                                                                                                                                                                                                                                                                                  |
| rate <1-100>                                                             | <p>Optional. Specifies the packet capture rate</p> <ul style="list-style-type: none"> <li>&lt;1-100&gt; – Specify a value from 1 - 100 seconds.</li> </ul>                                                                                                                                                                                                                                                                                                |
| snap <1-2048>                                                            | <p>Optional. Captures the data length</p> <ul style="list-style-type: none"> <li>&lt;1-2048&gt; – Specify a value from 1 - 2048 characters.</li> </ul>                                                                                                                                                                                                                                                                                                    |
| tcpdump                                                                  | Optional. Decodes the TCP dump                                                                                                                                                                                                                                                                                                                                                                                                                            |

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| verbose | Optional. Displays full packet body                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| write   | <p>Captures packets to a specified file. Provide the file name and location in the following format:</p> <ul style="list-style-type: none"> <li>flash:/path/file</li> <li>usbX:/path/file</li> </ul> <p>URL – Specify the location URL to capture file. Both IPv4 and IPv6 address formats are supported.</p> <ul style="list-style-type: none"> <li>nvrn:startup-config</li> <li>tftp://&lt;hostname IP&gt;[:port]/path/file</li> <li>ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IP&gt;[:port]/path/file</li> <li>sftp://&lt;user&gt;@&lt;hostname IP&gt;[:port]/path/file</li> <li>tzsp – TZSP (Tazman Sniffer Protocol) host. Specify the TZSP host's IP address or hostname.</li> </ul> |

```
service show last-passwd
```

|             |                                                                   |
|-------------|-------------------------------------------------------------------|
| show        | Displays running system statistics based on the parameters passed |
| last-passwd | Displays the last password used to enter shell                    |

```
service signal [abort <PROCESS-NAME>|kill <PROCESS-NAME>]
```

|        |                                                                                                                                                                                       |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| signal | <p>Sends a signal to a process</p> <ul style="list-style-type: none"> <li>tech-support – Copies extensive system information useful for troubleshooting</li> </ul>                    |
| abort  | <p>Sends an abort signal to a process, and forces it to dump to core</p> <ul style="list-style-type: none"> <li>&lt;PROCESS-NAME&gt; – Specify the process name.</li> </ul>           |
| kill   | <p>Sends a kill signal to a process, and forces it to terminate without a core</p> <ul style="list-style-type: none"> <li>&lt;PROCESS-NAME&gt; – Specify the process name.</li> </ul> |

```
service start-shell
```

|             |                       |
|-------------|-----------------------|
| start-shell | Provides shell access |
|-------------|-----------------------|

```
service trace <PROCESS-NAME> {summary}
```

|                |                                                             |
|----------------|-------------------------------------------------------------|
| trace          | Traces a process for system calls and signals               |
| <PROCESS-NAME> | Specifies the process name                                  |
| summary        | Optional. Generates summary report of the specified process |

### Syntax (Privilege Exec Mode: NX 95XX)

#### Service Commands - Intro

The following service commands are specific to the NX 95XX series service platforms:

```
service copy analytics-support [<FILE>|<URL>]
```



## Parameters(Privilege Exec Mode: NX 95XX)

### Service Commands - Intro

```
service copy analytics-support [<FILE>|<URL>]
```

|                        |                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| copy analytics-support | Enables copying of analytics information to a specified. Use one of the following options to specify the file:<br><br><b>Note:</b> This information is useful to troubleshoot issues by the Technical Support team.                                                                                                                                                    |
| <FILE>                 | Specify the file name and location using one of the following formats: <ul style="list-style-type: none"><li>• usb1:/path/file</li><li>• usb2:/path/file</li></ul>                                                                                                                                                                                                     |
| <URL>                  | Specify the location URL to copy file. Both IPv4 and IPv6 formats are supported. <ul style="list-style-type: none"><li>• tftp://&lt;hostname IPv4/IPv6&gt;[:port]/path/file</li><li>• ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IPv4/IPv6&gt;[:port]/path/file</li><li>• sftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IPv4/IPv6&gt;[:port]/path/file</li></ul> |

### Usage Guidelines

The NX 95XX and NX 96XX model service platforms (NOC) provide granular and robust analytic reporting for a managed network. The data analyzed is collected at intervals specified by the administrator.

To enable data analytics, procure and apply a separate hot spare analytics license at the NOC. The license restricts the number of Access Point streams processed at the NOC or forwarded to partner systems for further processing. The analytics feature can be turned on at select APs by enabling them in configuration. This way the customer can enable analytics on a select set of APs and not the entire system as long as the number of APs on which it is enabled is less than or equal to the total number of AP at the NOC controller.

In an NOC managed network, the analytics engine parses and processes Smart RF events as they are received. The analytics engine parses the new channel and power information from the Smart RF event, as opposed to retrieving the event from the devices themselves. analytics licenses available.

### Syntax (Global Config Mode)

#### Service Commands - Intro

```
service [set|show cli]
service set [command-history <10-300>|upgrade-history <10-100>|reboot-history <10-100>|
virtual-machine-history <10-200>] {on <DEVICE-NAME>}
service show cli
```

### Parameters (Global Config Mode)

#### Service Commands - Intro

```
service set [command-history <10-300>|upgrade-history <10-100>|reboot-history <10-100>|
virtual-machine-history <10-200>] {on <DEVICE-NAME>}
```

|                          |                                                                                                                                                                 |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| set                      | Sets the size of history files                                                                                                                                  |
| command-history <10-300> | Sets the size of the command history file <ul style="list-style-type: none"><li>• &lt;10-300&gt; – Specify a value from 10 - 300. The default is 200.</li></ul> |

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| upgrade-history<br><10-100>         | Sets the size of the upgrade history file <ul style="list-style-type: none"> <li>• &lt;10-100&gt; – Specify a value from 10 - 100. The default is 50.</li> </ul>                                                                                                                                                                                                                                                         |
| reboot-history<br><10-100>          | Sets the size of the reboot history file <ul style="list-style-type: none"> <li>• &lt;10-100&gt; – Specify a value from 10 - 100. The default is 50.</li> </ul>                                                                                                                                                                                                                                                          |
| virtual-machine-history<br><10-200> | Sets the size of the virtual-machine history file <ul style="list-style-type: none"> <li>• &lt;10-200&gt; – Specify a value from 10 - 200. The default is 100.</li> </ul> <p>This command is applicable only to the NX 95XX and NX 96XX series service platforms. Use the <b>no &gt; service &gt; set &gt; virtual-machine-history &gt; {on &lt;DEVICE-NAME&gt;}</b> command to revert the history file size to 100.</p> |
| on <DEVICE-NAME>                    | Optional. Sets the size of history files on a specified device <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul>                                                                                                                                                                                                           |

service show cli

|          |                                                                                                                                                   |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| show cli | Displays running system configuration details <ul style="list-style-type: none"> <li>• cli – Displays the CLI tree of the current mode</li> </ul> |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

### Service Commands - Intro

```

nx9500-6C8809>service show cli
Command mode: +-do
+-help [help]
 +-search
 +-WORD [help search WORD (|detailed|only-show|skip-show|skip-no)]
 +-detailed [help search WORD (|detailed|only-show|skip-show|skip-no)]
 +-only-show [help search WORD (|detailed|only-show|skip-show|skip-no)]
 +-skip-show [help search WORD (|detailed|only-show|skip-show|skip-no)]
 +-skip-no [help search WORD (|detailed|only-show|skip-show|skip-no)]
+-show
 +-commands [show commands]
 +-global
 +-device-list [show global device-list (|(filter {(online)|(offline)|(rf-domain (|not) RF-DOMAIN)})))]
 +-filter [show global device-list (|(filter {(online)|(offline)|(rf-domain (|not) RF-DOMAIN)})))]
 +-online [show global device-list (|(filter {(online)|(offline)|(rf-domain (|not) RF-DOMAIN)})))]
 +-offline [show global device-list (|(filter {(online)|(offline)|(rf-domain (|not) RF-DOMAIN)})))]
 +-rf-domain
 +-not
 +-RF-DOMAIN [show global device-list (|(filter {(online)|(offline)|(rf-domain (|not) RF-DOMAIN)})))]
 --More--
nx9500-6C8809>
nx9500-6C8809#service signal abort testprocess
Sending an abort signal to testprocess
nx9500-6C8809#
nx9500-6C8809#service show command-history on ap8132-74B45C
Configured size of command history is 200

 Date & Time User Location Command
=====
Nov 08 10:19:11 2017 admin 127.0.0.1 16 self

```

```

Nov 08 09:19:29 2017 admin 127.0.0.1 13 revert
Nov 08 09:18:52 2017 admin 127.0.0.1 13 interface radio 1
Nov 08 09:18:44 2017 admin 127.0.0.1 13 self
Nov 08 11:34:25 2017 admin 127.0.0.1 9 revert
Nov 08 11:34:06 2017 admin 127.0.0.1 9 self
Oct 06 07:15:18 2017 admin Console 6 self
Oct 06 07:15:01 2017 admin Console 6 self
Oct 06 07:14:17 2017 admin Console 6 wr mem
Oct 06 07:14:12 2017 admin Console 6 change-passwd
Oct 06 12:39:07 2017 admin Console 6 reload force
Oct 06 12:38:49 2017 admin Console 6 self
Oct 06 12:20:39 2017 admin Console 6 write memory
Oct 06 12:20:33 2017 admin Console 6 commit

```

--More--

```

nx9500-6C8809#
nx9500-6C8809#service show diag stats

```

```

fan 1 (System Fan 1) current speed: 2765 min_speed: 693 hysteresis: 250
fan 2 (System Fan 2) current speed: 3010 min_speed: 665 hysteresis: 250
fan 3 (System Fan 3) current speed: 2695 min_speed: 665 hysteresis: 250
fan 4 (System Fan 4) current speed: 3045 min_speed: 665 hysteresis: 250
fan 5 (System Fan 5) current speed: 6188 min_speed: 665 hysteresis: 250
fan 6 (System Fan 6) current speed: 5564 min_speed: 665 hysteresis: 250

```

```

Sensor 1 (Baseboard) Temperature 30.0 C
Sensor 2 (Front Panel) Temperature 20.0 C
Sensor 3 (PS1) Temperature 25.0 C
Sensor 4 (PS2) Temperature 27.0 C
Sensor 5 (HSBP) Temperature 21.0 C

```

```

nx9500-6C8809#
nx9500-6C8809#service show upgrade-history
Configured size of upgrade history is 50

```

| Date & Time          | Old Version  | New Version  | Status     |
|----------------------|--------------|--------------|------------|
| Feb 02 08:34:30 2018 | 5.9.2.0-007D | 5.9.2.0-008D | Successful |
| Jan 29 09:40:12 2018 | 5.9.2.0-005D | 5.9.2.0-007D | Successful |
| Jan 03 10:32:08 2018 | 5.9.1.0-029R | 5.9.2.0-005D | Successful |
| Sep 22 10:31:03 2017 | 5.9.1.0-026B | 5.9.1.0-029R | Successful |
| Sep 15 12:07:21 2017 | 5.9.1.0-025B | 5.9.1.0-026B | Successful |
| Sep 12 15:24:16 2017 | 5.9.1.0-025D | 5.9.1.0-025B | Successful |
| Sep 11 12:09:07 2017 | 5.9.1.0-024D | 5.9.1.0-025D | Successful |
| Sep 04 13:59:54 2017 | 5.9.1.0-023D | 5.9.1.0-024D | Successful |
| Sep 01 10:06:22 2017 | 5.9.1.0-022D | 5.9.1.0-023D | Successful |

--More--

```

nx9500-6C8809#
nx9500-6C8809#service show wireless reference reason-codes

```

| CODE | DESCRIPTION                                                             |
|------|-------------------------------------------------------------------------|
| 0    | Success                                                                 |
| 1    | Unspecified Reason                                                      |
| 2    | Previous authentication no longer valid                                 |
| 3    | Deauth because sending STA is leaving IBSS or ESS                       |
| 4    | Disassoc due to inactivity                                              |
| 5    | Disassoc because AP is unable to handle all currently assoc STA         |
| 6    | Class 2 frame received from non-authenticated STA                       |
| 7    | Class 3 frame received from nonassociated STA                           |
| 8    | Disassoc because STA is leaving BSS                                     |
| 9    | STA requesting association is not authentication with corresponding STA |
| 10   | Disassoc because info in the power capability elem is unacceptable      |
| 11   | Disassoc because info in the supp channels elem is unacceptable         |
| 12   | Reserved                                                                |

```

--More--
nx9500-6C8809#
nx9500-6C8809#service show wireless reference reason-codes
CODE DESCRIPTION
0 Success
1 Unspecified Reason
2 Previous authentication no longer valid
3 Deauth because sending STA is leaving IBSS or ESS
4 Disassoc due to inactivity
5 Disassoc because AP is unable to handle all currently assoc STA
6 Class 2 frame received from non-authenticated STA
7 Class 3 frame received from nonassociated STA
8 Disassoc because STA is leaving BSS
9 STA requesting association is not authentication with corresponding STA
10 Disassoc because info in the power capability elem is unacceptable
11 Disassoc because info in the supp channels elem is unacceptable
--More--
nx9500-6C8809#
nx9500-6C8809>service show wireless config-internal
! Startup-Config-Playback Completed: Yes
no debug wireless
country-code in
nx9500-6C8809>
nx9500-6C8809#service show wireless log-internal
08:51:49.417: wlan:Starting credcache checkup/sync (credcache.c:1539)
08:31:47.416: wlan:Starting credcache checkup/sync (credcache.c:1539)
08:11:42.415: wlan:Starting credcache checkup/sync (credcache.c:1539)
07:51:42.412: wlan:Starting credcache checkup/sync (credcache.c:1539)
07:31:42.412: wlan:Starting credcache checkup/sync (credcache.c:1539)
07:11:37.409: wlan:Starting credcache checkup/sync (credcache.c:1539)
06:51:36.408: wlan:Starting credcache checkup/sync (credcache.c:1539)
06:31:27.408: wlan:Starting credcache checkup/sync (credcache.c:1539)
06:11:24.408: wlan:Starting credcache checkup/sync (credcache.c:1539)
05:51:21.407: wlan:Starting credcache checkup/sync (credcache.c:1539)
05:31:18.406: wlan:Starting credcache checkup/sync (credcache.c:1539)
05:11:11.405: wlan:Starting credcache checkup/sync (credcache.c:1539)

--More--
nx9500-6C8809#
nx9500-6C8809#service show xpath-history

DATE&TIME USER
XPATH DURATION(MS)

Mon Feb 5 14:20:38 2018 system wing-stats/device/B4-C7-99-6C-88-09/upgrade-
history 10
Mon Feb 5 14:16:37 2018 system wing-stats/device/B4-C7-99-6C-88-09/service-
info 28
Mon Feb 5 14:15:11 2018 system wing-stats/device/B4-C7-99-6C-88-09/diag/
temp 449
Mon Feb 5 14:15:09 2018 system wing-stats/device/B4-C7-99-6C-88-09/diag/
fan 1748
Mon Feb 5 14:12:49 2018 system wing-stats/device/B4-C7-99-74-B4-5C/command-
history 49
Fri Feb 2 16:10:58 2018 system wing-stats/device/B4-C7-99-6C-88-09/content-filter/
web_filter_policy 0
--More--
nx9500-6C8809#

```

The following example shows the `service > show > virtual-machine-history` output on a NX9500 service platform:

```
nx9500-6C874D>service show virtual-machine-history
Configured size of virtual machine history is 100
```

```

 Date & Time Virtual Machine Event
=====
Jan 16 05:39:46 2017 Domain-0 autostart
Jan 10 03:47:09 2017 Domain-0 autostart
Jan 02 05:53:48 2017 Domain-0 autostart
Dec 27 10:52:59 2016 Domain-0 autostart
Oct 14 05:56:14 2016 Domain-0 autostart
Oct 14 03:01:48 2016 Domain-0 autostart
Oct 12 04:11:52 2016 Domain-0 autostart
Sep 30 04:41:08 2016 Domain-0 autostart
--More--
nx9500-6C874D>
```

Examples for the `service > wireless > meshpoint` command.

The following example displays meshpoint modules:

```
ROOT1-ap81xx-71174C#service wireless meshpoint z1 mesh_root on ROOT1-ap81xx-71174C
```

```

 | SUBZONE
 | 0 1 2 3 4 5 6 7
-----|-----
ZONE |
2-LLC | GEN TX RX BEA TXF
 | 0 0 0 0 0
3-ND | GEN TX RX NBR LQM LSA
 | 0 0 0 0 0 0
4-ORL | GEN
 | 0
5-LQ | GEN TX RX HEL PRO
 | 0 0 0 0 0
6-PS | GEN
 | 0
7-RS | GEN ROOT NBR REC
 | 0 0 0 0
8-IA | GEN
 | 0
11-MGT | GEN SET GET
 | 0 0 0
13-LSA | GEN RX TX R0 LMST LSUP LKEY KEY
 | 0 0 0 0 0 0 0 0
14-ACS | GEN SCAN TRIG
 | 0 0 0
15-EAP | GEN
 | 0
16-L2P | GEN
 | 0
```

```
ROOT1-ap81xx-71174C#
```

In the preceding example,

- The meshpoint name is `mesh_root`
- The device on which the command is executed is `ROOT1-ap81xx-71174C`
- The vertical ZONE column represents meshpoint modules. For example, 3-ND presents the Neighbor Discovery module.

- The SUBZONE 0 to 7 represents the available processes for each of the zonal modules.
- Debugging is disabled for all modules for the mesh-root meshpoint. A value of 0 (Zero) represents debugging disabled.

To enable meshpoint module debugging, specify the module number and the process number separated by a period (.). And then specify the debugging level from 0 - 7.

```
ROOT1-ap81xx-71174C#service wireless meshpoint z1 mesh_root on ROOT1-ap81xx-71174C 3.2 7
```

In the preceding command,

- The meshpoint module number provided is 3 (ND)
- The process number provided is 2 (RX - Received signals from neighbors)
- The debugging level provided is 7 (highest level - warning)

```
ROOT1-ap81xx-71174C#service wireless meshpoint z1 mesh_root on ROOT1-ap81xx-71174C
```

|        | SUBZONE |      |      |     |      |      |      |     |
|--------|---------|------|------|-----|------|------|------|-----|
|        | 0       | 1    | 2    | 3   | 4    | 5    | 6    | 7   |
| -----  |         |      |      |     |      |      |      |     |
| ZONE   |         |      |      |     |      |      |      |     |
| 2-LLC  | GEN     | TX   | RX   | BEA | TXF  |      |      |     |
|        | 0       | 0    | 0    | 0   | 0    |      |      |     |
| 3-ND   | GEN     | TX   | RX   | NBR | LQM  | LSA  |      |     |
|        | 0       | 0    | 7(D) | 0   | 0    | 0    |      |     |
| 4-ORL  | GEN     |      |      |     |      |      |      |     |
|        | 0       |      |      |     |      |      |      |     |
| 5-LQ   | GEN     | TX   | RX   | HEL | PRO  |      |      |     |
|        | 0       | 0    | 0    | 0   | 0    |      |      |     |
| 6-PS   | GEN     |      |      |     |      |      |      |     |
|        | 0       |      |      |     |      |      |      |     |
| 7-RS   | GEN     | ROOT | NBR  | REC |      |      |      |     |
|        | 0       | 0    | 0    | 0   |      |      |      |     |
| 8-IA   | GEN     |      |      |     |      |      |      |     |
|        | 0       |      |      |     |      |      |      |     |
| 11-MGT | GEN     | SET  | GET  |     |      |      |      |     |
|        | 0       | 0    | 0    |     |      |      |      |     |
| 13-LSA | GEN     | RX   | TX   | R0  | LMST | LSUP | LKEY | KEY |
|        | 0       | 0    | 0    | 0   | 0    | 0    | 0    | 0   |
| 14-ACS | GEN     | SCAN | TRIG |     |      |      |      |     |
|        | 0       | 0    | 0    |     |      |      |      |     |
| 15-EAP | GEN     |      |      |     |      |      |      |     |
|        | 0       |      |      |     |      |      |      |     |
| 16-L2P | GEN     |      |      |     |      |      |      |     |
|        | 0       |      |      |     |      |      |      |     |

```
ROOT1-ap81xx-71174C#
```

In the preceding example, level 7 debugging has been enabled only for the ND module's received signals. Note that debugging for all other modules and processes are still disabled.

To disable debugging for all modules, specify 0 (zero) in the command. For example:

```
ROOT1-ap81xx-71174C#service wireless meshpoint z1 mesh_root on ROOT1-ap81xx-71174C 0
```

To enable debugging for all modules, specify the debugging level number. For example:

```
ROOT1-ap81xx-71174C#service wireless meshpoint z1 mesh_root on ROOT1-ap81xx-71174C 5
```

```
ROOT1-ap81xx-71174C#service wireless meshpoint z1 mesh_root on ROOT1-ap81xx-71174C
```

|       | SUBZONE |      |      |      |      |   |   |   |
|-------|---------|------|------|------|------|---|---|---|
|       | 0       | 1    | 2    | 3    | 4    | 5 | 6 | 7 |
| ----- |         |      |      |      |      |   |   |   |
| ZONE  |         |      |      |      |      |   |   |   |
| 2-LLC | GEN     | TX   | RX   | BEA  | TXF  |   |   |   |
|       | 5(N)    | 5(N) | 5(N) | 5(N) | 5(N) |   |   |   |

```

 | GEN TX RX NBR LQM LSA
3-ND | 5(N) 5(N) 5(N) 5(N) 5(N) 5(N)
 | GEN
4-ORL | 5(N)
 | GEN TX RX HEL PRO
5-LQ | 5(N) 5(N) 5(N) 5(N) 5(N)
 | GEN
6-PS | 5(N)
 | GEN ROOT NBR REC
7-RS | 5(N) 5(N) 5(N) 5(N)
 | GEN
8-IA | 5(N)
 | GEN SET GET
11-MGT | 5(N) 5(N) 5(N)
 | GEN RX TX R0 LMST LSUP LKEY KEY
13-LSA | 5(N) 5(N) 5(N) 5(N) 5(N) 5(N) 5(N) 5(N)
 | GEN SCAN TRIG
14-ACS | 5(N) 5(N) 5(N)
 | GEN
15-EAP | 5(N)
 | GEN
16-L2P | 5(N)

```

```
ROOT1-ap81xx-71174C#
```

```

rfs4000-1BE644#service show ssh-authorized-keys
'extreme@extreme-quadcore'
rfs4000-1BE644#
rfs4000-1BE644#service load-ssh-authorized-keys "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDPERY9aTibRY1FMnERTYP2iyylJ00YELxjUEly7Zm9Ky2yeSmgl5UKerJ
+IP161Gdm0AoEfXyeheRntK
+Z6NWHa341RWJ0UrQMcp7hSEE5jbDpLKJOUeEoW22Ag45BZzMV7EnM7lHowboNsQhSzX5uBB1VViWlBxBqDroX4BcuB/
CFugezHTt95UQ2ZRUFHvePS6jQdOArflalwk0Slcsz4HNSl5KDutJ4VY+6vRvlf5Gy/
3GNehMwNsmsRKK4UVKV5RpuuKIjkbZE+goPFAKYVPNmZngjaOyDfvNGE7JIwmYlti/
AId6tv2zAbM4qSomWAgU000hkXS9m4m74FnHPr extreme@extreme-quadcore"
Successfully added the ssh key
rfs4000-1BE644#
rfs4000-1BE644#no service load-ssh-authorized-keys rfs4000-1BE644
Successfully removed the ssh key
rfs4000-1BE644#
nx9500-6C8809#service show diag fds
Process open fds
cfgd 86
nx9500-6C8809#
nx9500-6C8809#service show diag pkts
Date: 11-4-2016, Time: 8:41:08.501033, Len: 64, 802.3, Proto: 0x8783, Vlan: 1, Priority:
0, Ingress: gel, vlan1
Loop reason: Unknown(540)
TRUNCATED BB-7C-4D-80-C2-AC > 10-01-00-D2-68-99 at 64 bytes

Date: 11-4-2016, Time: 8:41:08.707631, Len: 64, 802.3, Proto: 0x8783, Vlan: 1, Priority:
0, Ingress: gel, vlan1
Loop reason: Unknown(540)
TRUNCATED BB-7C-4D-80-C2-AC > 10-01-00-D2-68-99 at 64 bytes

Date: 11-4-2016, Time: 8:41:08.830963, Len: 64, 802.3, Proto: 0x8783, Vlan: 1, Priority:
0, Ingress: gel, vlan1
Loop reason: Unknown(540)
TRUNCATED BB-7C-4D-83-30-A4 > 10-01-00-42-68-99 at 64 bytes

```

```

--More--
nx9500-6C8809#
nx9500-6C8809#service clear diag pkts
nx9500-6C8809#service show diag pkts
nx9500-6C8809#
nx9500-6C8809#service show diag psu
PSU1 (upper):
 status unplugged
PSU2 (lower):
 status normal
nx9500-6C8809#

```

The following examples show the purging of users from the guest-registration database:

```

nx7500-112233#service guest-registration delete ?
 all Delete all users
 email Email address
 group Group
 mac MAC address
 mobile Mobile phone number
 name Full name
 offline-for Specify minimum amount of time offline
 otp-incomplete-for Specify minimum amount of time registration with
 one-time-passcode incomplete
 social Social site used to log in
 wlan Wireless LAN

nx7500-112233#

```

Purges users belonging to a specified RADIUS group.

```

nx7500-112233#service guest-registration delete group mac_reg_gr1
delete user status: delete users matching a group will take time, please wait
nx7500-112233#

```

Purges users using social-site (Facebook or Google) credentials to login.

```

nx7500-112233#service guest-registration delete social facebook
delete user status: delete users matching a social category will take time, please wait
nx7500-112233#

```

Purges users inactive for a specified time period.

```

nx7500-112233#service guest-registration delete offline-for days 5
delete user status: Deleting users offline for minimum 5 days. This will take time, please
wait
nx7500-112233#

```

Purges users who have failed to complete registration using the OTP within a specified time period.

```

nx7500-112233#service guest-registration delete otp-incomplete-for days 5
delete user status: Deleting registration with one-time-passcode incomplete for minimum 5
days. This will take time, please wait
nx7500-112233#

```

The following example displays IP ACLs to WLAN mapping summary on the 'TechPubs' RF Domain:

```

nx9500-6C8809#service show ip-access-list wlan TechPubs status
Reporting Device: ap7161-99BE7C - success
Reporting Device: ap7532-80C2AC - success
Reporting Device: ap7562-84A224 - success
Reporting Device: nx9500-6C8809 - success
Reporting Device: ap8163-74B45C - success
Total reporting devices: 5
nx9500-6C8809#

```



Consider an RF Domain (name guest-domain) with 3 APs adopted to a controller. The CLI output for the **service > show > ip-access-list** command in this set up varies for different scenarios, as shown in the following examples:

- Scenario 1: Executing the command on a device (access point).

```
AP01#service show ip-access-list wlan status
Reporting Device: AP01 - fail
WLAN: XPO-Guest-PSK
 use ip-access-list in guest_access_inbound : fail
Total reporting devices: 1
AP01#

AP01#service show ip-access-list wlan status detail
=====
Reporting Device: AP01

WLAN: XPO-Guest-PSK
 use ip-access-list in guest_access_inbound : fail
 use ip-access-list out BC-MC-CONTROL : success

WLAN: PartnerNet
 use ip-access-list in default : success
 use ip-access-list out default : success

Total reporting devices: 1
AP01#
```

- Scenario 2: IP ACL to WLAN mapping is successful for all APs in a specified RF Domain.

```
SW01#service show ip-access-list wlan status on guest-domain
Reporting Device: AP01 - success
Reporting Device: AP02 - success
Reporting Device: AP03 - success
Total reporting devices: 3
SW01#
```

- Scenario 3: IP ACL has failed in dataplane due to unknown reasons.

```
SW01#service show ip-access-list wlan status on guest-domain
Reporting Device: AP01 - fail
WLAN: XPO-Guest-PSK
 use ip-access-list in guest_access_inbound : fail
Reporting Device: AP02 - success
Reporting Device: AP03 - success
Total reporting devices: 3
SW01#

SW01#service show ip-access-list wlan status detail on guest-domain
=====
Reporting Device: AP01

WLAN: XPO-Guest-PSK
 use ip-access-list in guest_access_inbound : fail
 use ip-access-list out BC-MC-CONTROL : success

WLAN: PartnerNet
 use ip-access-list in guest_access_inbound : success
 use ip-access-list out BC-MC-CONTROL : success

=====
Reporting Device: AP02

WLAN: PartnerNet
 use ip-access-list in guest_access_inbound : success
 use ip-access-list out BC-MC-CONTROL : success

```

```

=====
Reporting Device: AP03

WLAN: PartnerNet
 use ip-access-list in guest_access_inbound : success
 use ip-access-list out BC-MC-CONTROL : success

Total reporting devices: 3
SW01#

```

- Scenario 4: AP in RF Domain is unreachable or does not support this functionality.

```

SW01#service show ip-access-list wlan status on guest-domain
Reporting Device: AP01 - unreachable
Reporting Device: AP02 - success
Reporting Device: AP03 - success
Total reporting devices: 3
SW01#
SW01#service show ip-access-list wlan status detail on guest-domain
=====
Reporting Device: AP01
Timed out waiting for remote device: xpath=wing-stats/device/00-23-68-0B-86-38/firewall/
ip_acl_intf_status/wlan[mac='*']
=====
Reporting Device: AP02

WLAN: PartnerNet
 use ip-access-list in guest_access_inbound : success
 use ip-access-list out BC-MC-CONTROL : success

Reporting Device: AP03

WLAN: PartnerNet
 use ip-access-list in guest_access_inbound : success
 use ip-access-list out BC-MC-CONTROL : success

Total reporting devices: 3
SW01#

```

## show

Displays specified system component settings. There are a number of ways to invoke the show command.

- When invoked without any arguments, it displays information about the current context. If the current context contains instances, the show command (usually) displays a list of these instances.
- When invoked with the display parameter, it displays information about that component.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show <PARAMETERS>
```

## Parameters

show <PARAMETERS>

|                   |                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show <PARAMETERS> | The show command displays configuration details based on the configuration mode, in which the command is executed, and the parameters passed. For example, when executed in the AAA policy configuration mode, it displays the logged AAA policy's current settings. The example below shows the configuration details that can be viewed in the Priv Executable mode. |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809#show ?
adoption Adoption related information
bluetooth Bluetooth Configuration/Statistics commands
bonjour Bonjour Gateway related commands
boot Display boot configuration.
captive-portal Captive portal commands
captive-portal-page-upload Captive portal internal and advanced page upload
cdp Cisco Discovery Protocol
classify-url Query the category of an URL
clock Display system clock
cluster Cluster Protocol
cmp-factory-certs Display the CMP certificate status
commands Show command lists
context Information about current context
critical-resources Critical Resources
crypto Encryption related commands
database Database
debug Debugging functions
debugging Debugging functions
device-upgrade Device Upgrade
dot1x 802.1X
dpi Deep Packet Inspection
eguest Registration EGuest process
environmental-sensor Display Environmental Sensor Module status
event-history Display event history
event-system-policy Display event system policy
ex3500 EX3500 device details
extdev External device (T5, Ex3500..)
file Display filesystem information
file-sync File sync between controller and adoptees
firewall Wireless Firewall
global Global-level information
gre Show l2gre tunnel info
guest-notification-config Show guest-notification information
guest-registration Guest registration commands
interface Interface Configuration/Statistics commands
ip Internet Protocol (IP)
ip-access-list IP ACL
ipv6 Internet Protocol version 6 (IPv6)
ipv6-access-list IPV6 ACL
l2tpv3 L2TPv3 information
lacp LACP commands
ldap-agent LDAP Agent Configuration
licenses Show installed licenses and usage
lldp Link Layer Discovery Protocol
logging Show logging information
mac-access-list MAC ACL
mac-address-table Display MAC address table
mac-auth MAC authentication
mac-auth-clients MAC authenticated clients
mint MiNT protocol
mirroring Show mirroring sessions
```

|                     |                                                                                |
|---------------------|--------------------------------------------------------------------------------|
| nsight              | Nsight Server Module                                                           |
| ntp                 | Network time protocol                                                          |
| password-encryption | Pasword encryption                                                             |
| pppoe-client        | PPP Over Ethernet client                                                       |
| privilege           | Show current privilege level                                                   |
| radius              | RADIUS statistics commands                                                     |
| raid                | Show RAID status                                                               |
| reload              | Scheduled reload information                                                   |
| remote-debug        | Show details of remote debug sessions                                          |
| rf-domain-manager   | Show RF Domain Manager selection details                                       |
| role                | Role based firewall                                                            |
| route-maps          | Display Route Map Statistics                                                   |
| rtls                | RTLS Statistics                                                                |
| running-config      | Current operating configuration                                                |
| session-changes     | Configuration changes made in this session                                     |
| session-config      | This session configuration                                                     |
| sessions            | Display sessions                                                               |
| site-config-diff    | Difference between site configuration on the NOC and actual site configuration |
| slot                | Expansion slots stats                                                          |
| smart-rf            | Smart-RF Management Commands                                                   |
| spanning-tree       | Display spanning tree information                                              |
| startup-config      | Startup configuration                                                          |
| t5                  | Display T5 inventory information                                               |
| terminal            | Display terminal configuration parameters                                      |
| timezone            | The timezone                                                                   |
| traffic-shape       | Display traffic shaping                                                        |
| upgrade-status      | Display last image upgrade status                                              |
| version             | Display software & hardware version                                            |
| virtual-machine     | Virtual Machine                                                                |
| vrrp                | VRRP protocol                                                                  |
| web-filter          | Web filter                                                                     |
| what                | Perform global search                                                          |
| wireless            | Wireless commands                                                              |
| wwan                | Display wireless WAN Status                                                    |

nx9500-6C8809#



**Note**

For more information on the show command, see [SHOW COMMANDS](#).

*write*

Writes the system running configuration to memory or terminal

**Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

**Syntax**

`write [memory|terminal]`

**Parameters**

`write [memory|terminal]`

---

|          |                                        |
|----------|----------------------------------------|
| memory   | Writes to the NV (non-volatile) memory |
| terminal | Writes to the terminal                 |

### Examples

```
nx9500-6C8809>write memory
[OK]
nx9500-6C8809>
```

# SHOW COMMANDS

## SHOW COMMANDS

---

Show commands displays configuration settings and statistical information. Use this command to view the current running configuration as well as the start-up configuration. The show command also displays the current context configuration.

This chapter describes the 'show' CLI commands used in the USER EXEC, PRIV EXEC, and GLOBAL CONFIG modes. Commands entered in either USER EXEC mode or PRIV EXEC mode are referred to as EXEC mode commands. If a user or privilege is not specified, the referenced command can be entered in either mode.

This chapter also describes the 'show' commands in the 'GLOBAL CONFIG' mode. The commands can be entered in all three modes, except commands like file, IP access list statistics, MAC access list statistics, and upgrade statistics, which cannot be entered in the USER EXEC mode.

### show-commands

The following table summarizes the show commands:

*Table: Show Commands*

| Command                                       | Description                                                                                                           |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <a href="#">show</a>                          | Displays settings for the specified system component                                                                  |
| <a href="#">adoption</a>                      | Displays adoption related information                                                                                 |
| <a href="#">bluetooth</a> on page 709         | Displays Bluetooth radio statistics for RF Domain member access points                                                |
| <a href="#">boot</a>                          | Displays a device boot configuration                                                                                  |
| <a href="#">bonjour</a> on page 712           | Displays the configured Bonjour services available on local and remote sites                                          |
| <a href="#">captive-portal</a>                | Displays WLAN hotspot functions                                                                                       |
| <a href="#">captive-portal-page-upload</a>    | Displays captive portal Web pages upload related information                                                          |
| <a href="#">cdp</a>                           | Displays a CDP (Cisco Discovery Protocol ) neighbor table                                                             |
| <a href="#">classify-url</a> on page 717      | Queries a specified global data center or a pre-configured classification server for the category of a specified URL. |
| <a href="#">clock</a>                         | Displays the system clock                                                                                             |
| <a href="#">cluster</a>                       | Displays device-cluster related statistics                                                                            |
| <a href="#">cmp-factory-certs</a> on page 719 | Displays factory installed CMP certificates                                                                           |
| <a href="#">commands</a>                      | Displays command list                                                                                                 |
| <a href="#">context</a>                       | Displays information about the current context                                                                        |
| <a href="#">critical-resources</a>            | Displays critical resources deployed within the managed network and associated statistics                             |

| Command                                              | Description                                                                                                                                                                                        |
|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">crypto</a>                               | Displays encryption mode information                                                                                                                                                               |
| <a href="#">database</a> on page 724                 | Displays database-related statistics and status                                                                                                                                                    |
| <a href="#">device-upgrade</a>                       | Displays device firmware upgradation information for devices adopted by a wireless controller or access point                                                                                      |
| <a href="#">dot1x</a>                                | Displays dot1x information on interfaces                                                                                                                                                           |
| <a href="#">dpi</a> on page 730                      | Displays statistics for all configured and canned applications                                                                                                                                     |
| <a href="#">eguest</a> on page 732                   | Displays EGuest server status and EGuest registration statistics                                                                                                                                   |
| <a href="#">environmental-sensor</a>                 | Displays environmental sensor's historical data (applicable only to AP 8132)                                                                                                                       |
| <a href="#">event-history</a>                        | Displays event history                                                                                                                                                                             |
| <a href="#">event-system-policy</a>                  | Displays event system policy configuration information                                                                                                                                             |
| <a href="#">ex3500</a> on page 737                   | Displays EX3500-related statistical data                                                                                                                                                           |
| <a href="#">extdev</a> on page 740                   | Displays external device (T5 or EX3500) configuration error history                                                                                                                                |
| <a href="#">fabric-attach</a> on page 740            | Displays the current status of VLAN to I-SID assignments for all ports                                                                                                                             |
| <a href="#">file</a>                                 | Displays file system information                                                                                                                                                                   |
| <a href="#">file-sync</a> on page 742                | Displays file synchronization settings and status on a controller. The file-sync command syncs trustpoint/wireless-bridge certificate between the staging-controller and its adopted access points |
| <a href="#">firewall</a>                             | Displays wireless firewall information                                                                                                                                                             |
| <a href="#">global</a>                               | Displays global information for network devices based on the parameters passed                                                                                                                     |
| <a href="#">gre</a>                                  | Displays GRE tunnel related information                                                                                                                                                            |
| <a href="#">guest-registration</a> on page 750       | Displays guest registration statistics based on the option and time entered                                                                                                                        |
| <a href="#">interface</a>                            | Displays interface status                                                                                                                                                                          |
| <a href="#">iot-device-type-imagotag</a> on page 759 | Displays the configuration of ESL communicator on a specified AP or on all APs within an RF Domain.                                                                                                |
| <a href="#">ip</a>                                   | Displays IP related information                                                                                                                                                                    |
| <a href="#">ip-access-list-stats</a>                 | Displays IP access list statistics                                                                                                                                                                 |
| <a href="#">ipv6</a> on page 768                     | Displays IPv6 related information                                                                                                                                                                  |
| <a href="#">ipv6-access-list</a> on page 771         | Displays IPv6 access list statistics                                                                                                                                                               |
| <a href="#">l2tpv3</a>                               | Displays L2TPv3 (Layer 2 Tunnel Protocol Version 3) information                                                                                                                                    |
| <a href="#">lACP</a> on page 774                     | Displays LACP (Link Aggregation Control Protocol) related information                                                                                                                              |
| <a href="#">ldap-agent</a>                           | Displays an LDAP agent's join status (join status to a LDAP server domain)                                                                                                                         |
| <a href="#">licenses</a>                             | Displays installed licenses and usage information                                                                                                                                                  |
| <a href="#">lldp</a>                                 | Displays LLDP ( <i>Link Layer Discovery Protocol</i> ) information                                                                                                                                 |
| <a href="#">logging</a>                              | Displays logging information                                                                                                                                                                       |
| <a href="#">mac-access-list-stats</a>                | Displays MAC access list statistics                                                                                                                                                                |

| Command                                         | Description                                                                                                                                                                                                 |
|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">mac-address-table</a>               | Displays MAC address table entries                                                                                                                                                                          |
| <a href="#">macauth</a> on page 782             | Displays details of wired ports that have MAC address-based authentication enabled                                                                                                                          |
| <a href="#">mac-auth-clients</a> on page 783    | Displays MAC-authenticated clients based on the parameters passed                                                                                                                                           |
| <a href="#">mint</a>                            | Displays MiNT protocol configuration commands                                                                                                                                                               |
| <a href="#">nsight</a> on page 787              | Displays NSight module related statistics and also displays the database server status (reachable or not)                                                                                                   |
| <a href="#">ntp</a>                             | Displays NTP server related information                                                                                                                                                                     |
| <a href="#">password-encryption</a> on page 789 | Displays password encryption status                                                                                                                                                                         |
| <a href="#">pppoe-client</a>                    | Displays PPPoE (Point to Point Protocol over Ethernet) client information                                                                                                                                   |
| <a href="#">privilege</a>                       | Displays current privilege level information                                                                                                                                                                |
| <a href="#">radius</a> on page 791              | Displays the amount of access time consumed and the access time remaining for all guest users configured on a RADIUS server                                                                                 |
| <a href="#">reload</a>                          | Displays scheduled reload information                                                                                                                                                                       |
| <a href="#">rf-domain-manager</a>               | Displays RF Domain manager selection details                                                                                                                                                                |
| <a href="#">role</a>                            | Displays role-based firewall information                                                                                                                                                                    |
| <a href="#">route-maps</a>                      | Display route map statistics                                                                                                                                                                                |
| <a href="#">rtls</a>                            | Displays RTLS (Real Time Location Service) statistics of Access Points                                                                                                                                      |
| <a href="#">running-config</a>                  | Displays configuration file contents                                                                                                                                                                        |
| <a href="#">session-changes</a>                 | Displays configuration changes made in the current session                                                                                                                                                  |
| <a href="#">session-config</a>                  | Displays configurations made in the current session                                                                                                                                                         |
| <a href="#">sessions</a>                        | Displays a list of currently active open sessions on the device                                                                                                                                             |
| <a href="#">site-config-diff</a>                | Displays the difference between site configuration available on NOC and the actual site configuration                                                                                                       |
| <a href="#">smart-rf</a>                        | Displays Smart RF management statistics                                                                                                                                                                     |
| <a href="#">spanning-tree</a>                   | Displays spanning tree information                                                                                                                                                                          |
| <a href="#">startup-config</a>                  | Displays complete startup configuration script on the console                                                                                                                                               |
| <a href="#">t5</a> on page 814                  | Displays adopted T5 controller details. This command is applicable only on the RFS 4000, NX 95XX, NX 96XX, and VX 9000.                                                                                     |
| <a href="#">terminal</a> on page 822            | Displays terminal configuration parameters                                                                                                                                                                  |
| <a href="#">timezone</a>                        | Displays timezone information for the system and managed devices                                                                                                                                            |
| <a href="#">traffic-shape</a> on page 822       | Displays traffic-shaping related configuration details and statistics                                                                                                                                       |
| <a href="#">upgrade-status</a>                  | Displays image upgrade status                                                                                                                                                                               |
| <a href="#">version</a>                         | Displays a device's software and hardware version                                                                                                                                                           |
| <a href="#">vrrp</a>                            | Displays VRRP (Virtual Router Redundancy Protocol) protocol details                                                                                                                                         |
| <a href="#">web-filter</a> on page 829          | Displays pre-configured, in-built Web filter options available. These options are: category (URL category), category-types, filter-level, etc. This command also displays Web filter statistics and status. |



| Command                           | Description                                                           |
|-----------------------------------|-----------------------------------------------------------------------|
| <code>what</code>                 | Displays details of a specified search phrase                         |
| <code>wireless</code> on page 831 | Displays wireless configuration parameters                            |
| <code>wwan</code>                 | Displays the wireless WAN status                                      |
| <code>virtual-machine</code>      | Displays the virtual-machine (VM) configuration, logs, and statistics |



#### Note

The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore ( \_ ) character. In other words, the name of a device cannot contain an underscore.

## show

The show command displays the following information:

- A device's current configuration
- A device's start-up configuration
- A device's current context configuration, such as profiles and policies

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
show <PARAMETER>
```

#### Parameters

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show <PARAMETERS> | The show command displays configuration details based on the configuration mode, in which the command is executed, and the parameters passed. For example, when executed in the AAA policy configuration mode, it displays the logged AAA policy's current settings. The examples below show the configuration parameters that can be viewed in the User Executable, Priv Executable, and Global Configurable modes. |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

The following examples list the *show* commands in the User Exec, Priv Exec, and Global Config modes:

#### Global Config Mode:

```
<DEVICE>(config)#show ?
 adoption Adoption related information
 bluetooth Bluetooth Configuration/Statistics commands
 bonjour Bonjour Gateway related commands
 boot Display boot configuration.
 captive-portal Captive portal commands
 captive-portal-page-upload Captive portal internal and advanced page upload
 cdp Cisco Discovery Protocol
 classify-url Query the category of an URL
 clock Display system clock
```

|                           |                                                                                |
|---------------------------|--------------------------------------------------------------------------------|
| cluster                   | Cluster Protocol                                                               |
| cmp-factory-certs         | Display the CMP certificate status                                             |
| commands                  | Show command lists                                                             |
| context                   | Information about current context                                              |
| critical-resources        | Critical Resources                                                             |
| crypto                    | Encryption related commands                                                    |
| database                  | Database                                                                       |
| debug                     | Debugging functions                                                            |
| debugging                 | Debugging functions                                                            |
| device-upgrade            | Device Upgrade                                                                 |
| dot1x                     | 802.1X                                                                         |
| dpi                       | Deep Packet Inspection                                                         |
| eguest                    | ExtremeGuest                                                                   |
| environmental-sensor      | Display Environmental Sensor Module status                                     |
| event-history             | Display event history                                                          |
| event-system-policy       | Display event system policy                                                    |
| ex3500                    | EX3500 device details                                                          |
| extdev                    | External device (T5, Ex3500..)                                                 |
| fabric-attach             | Fabric attach                                                                  |
| file                      | Display filesystem information                                                 |
| file-sync                 | File sync between controller and adoptees                                      |
| firewall                  | Wireless Firewall                                                              |
| global                    | Global-level information                                                       |
| gre                       | Show l2gre tunnel info                                                         |
| guest-notification-config | Show guest-notification information                                            |
| guest-registration        | Guest registration commands                                                    |
| interface                 | Interface Configuration/Statistics commands                                    |
| iot-device-type-imagotag  | Iot device type imagotag                                                       |
| ip                        | Internet Protocol (IP)                                                         |
| ip-access-list            | IP ACL                                                                         |
| ipv6                      | Internet Protocol version 6 (IPv6)                                             |
| ipv6-access-list          | IPv6 ACL                                                                       |
| l2tpv3                    | L2TPv3 information                                                             |
| lacp                      | LACP commands                                                                  |
| ldap-agent                | LDAP Agent Configuration                                                       |
| licenses                  | Show installed licenses and usage                                              |
| lldp                      | Link Layer Discovery Protocol                                                  |
| logging                   | Show logging information                                                       |
| mac-access-list           | MAC ACL                                                                        |
| mac-address-table         | Display MAC address table                                                      |
| mac-auth                  | MAC authentication                                                             |
| mac-auth-clients          | MAC authenticated clients                                                      |
| mint                      | MiNT protocol                                                                  |
| mirroring                 | Show mirroring sessions                                                        |
| nsight                    | Nsight Server Module                                                           |
| ntp                       | Network time protocol                                                          |
| password-encryption       | Pasword encryption                                                             |
| pppoe-client              | PPP Over Ethernet client                                                       |
| privilege                 | Show current privilege level                                                   |
| radius                    | RADIUS statistics commands                                                     |
| raid                      | Show RAID status                                                               |
| reload                    | Scheduled reload information                                                   |
| remote-debug              | Show details of remote debug sessions                                          |
| rf-domain-manager         | Show RF Domain Manager selection details                                       |
| role                      | Role based firewall                                                            |
| route-maps                | Display Route Map Statistics                                                   |
| rtls                      | RTLS Statistics                                                                |
| running-config            | Current operating configuration                                                |
| session-changes           | Configuration changes made in this session                                     |
| session-config            | This session configuration                                                     |
| sessions                  | Display sessions                                                               |
| site-config-diff          | Difference between site configuration on the NOC and actual site configuration |
| slot                      | Expansion slots stats                                                          |

|                 |                                           |
|-----------------|-------------------------------------------|
| smart-rf        | Smart-RF Management Commands              |
| spanning-tree   | Display spanning tree information         |
| startup-config  | Startup configuration                     |
| t5              | Display T5 inventory information          |
| terminal        | Display terminal configuration parameters |
| timezone        | The timezone                              |
| traffic-shape   | Display traffic shaping                   |
| upgrade-status  | Display last image upgrade status         |
| version         | Display software & hardware version       |
| virtual-machine | Virtual Machine                           |
| vrrp            | VRRP protocol                             |
| web-filter      | Web filter                                |
| what            | Perform global search                     |
| wireless        | Wireless commands                         |
| wwan            | Display wireless WAN Status               |

```
<DEVICE>(config)#
rfs4000-6DB5D4(config)#show clock
2018-02-06 09:26:53 IST
rfs4000-6DB5D4(config)#
```

### Privilege Executable Mode:

```
<DEVICE>#show ?
adoption Adoption related information
bluetooth Bluetooth Configuration/Statistics commands
bonjour Bonjour Gateway related commands
boot Display boot configuration.
captive-portal Captive portal commands
captive-portal-page-upload Captive portal internal and advanced page upload
cdp Cisco Discovery Protocol
classify-url Query the category of an URL
clock Display system clock
cluster Cluster Protocol
cmp-factory-certs Display the CMP certificate status
commands Show command lists
context Information about current context
critical-resources Critical Resources
crypto Encryption related commands
database Database
debug Debugging functions
debugging Debugging functions
device-upgrade Device Upgrade
dot1x 802.1X
dpi Deep Packet Inspection
eguest ExtremeGuest
environmental-sensor Display Environmental Sensor Module status
event-history Display event history
event-system-policy Display event system policy
ex3500 EX3500 device details
extdev External device (T5, Ex3500..)
fabric-attach Fabric attach
file Display filesystem information
file-sync File sync between controller and adoptees
firewall Wireless Firewall
global Global-level information
gre Show l2gre tunnel info
guest-notification-config Show guest-notification information
guest-registration Guest registration commands
interface Interface Configuration/Statistics commands
ip Internet Protocol (IP)
iot-device-type-imagotag Iot device type imagotag
ip-access-list IP ACL
ipv6 Internet Protocol version 6 (IPv6)
```

|                     |                                                                                |
|---------------------|--------------------------------------------------------------------------------|
| ipv6-access-list    | IPv6 ACL                                                                       |
| l2tpv3              | L2TPv3 information                                                             |
| lacp                | LACP commands                                                                  |
| ldap-agent          | LDAP Agent Configuration                                                       |
| licenses            | Show installed licenses and usage                                              |
| lldp                | Link Layer Discovery Protocol                                                  |
| logging             | Show logging information                                                       |
| mac-access-list     | MAC ACL                                                                        |
| mac-address-table   | Display MAC address table                                                      |
| mac-auth            | MAC authentication                                                             |
| mac-auth-clients    | MAC authenticated clients                                                      |
| mint                | MiNT protocol                                                                  |
| mirroring           | Show mirroring sessions                                                        |
| nsight              | Nsight Server Module                                                           |
| ntp                 | Network time protocol                                                          |
| password-encryption | Password encryption                                                            |
| pppoe-client        | PPP Over Ethernet client                                                       |
| privilege           | Show current privilege level                                                   |
| radius              | RADIUS statistics commands                                                     |
| raid                | Show RAID status                                                               |
| reload              | Scheduled reload information                                                   |
| remote-debug        | Show details of remote debug sessions                                          |
| rf-domain-manager   | Show RF Domain Manager selection details                                       |
| role                | Role based firewall                                                            |
| route-maps          | Display Route Map Statistics                                                   |
| rtls                | RTLS Statistics                                                                |
| running-config      | Current operating configuration                                                |
| session-changes     | Configuration changes made in this session                                     |
| session-config      | This session configuration                                                     |
| sessions            | Display sessions                                                               |
| site-config-diff    | Difference between site configuration on the NOC and actual site configuration |
| slot                | Expansion slots stats                                                          |
| smart-rf            | Smart-RF Management Commands                                                   |
| spanning-tree       | Display spanning tree information                                              |
| startup-config      | Startup configuration                                                          |
| t5                  | Display T5 inventory information                                               |
| terminal            | Display terminal configuration parameters                                      |
| timezone            | The timezone                                                                   |
| traffic-shape       | Display traffic shaping                                                        |
| upgrade-status      | Display last image upgrade status                                              |
| version             | Display software & hardware version                                            |
| virtual-machine     | Virtual Machine                                                                |
| vrrp                | VRRP protocol                                                                  |
| web-filter          | Web filter                                                                     |
| what                | Perform global search                                                          |
| wireless            | Wireless commands                                                              |
| wwan                | Display wireless WAN Status                                                    |

```
<DEVICE>#
nx9500-6C8809#show terminal
Terminal Type: xterm
Length: 24 Width: 80
nx9500-6C8809#
```

### User Executable Mode:

```
<DEVICE>>show ?
 adoption Adoption related information
 bluetooth Bluetooth Configuration/Statistics commands
 bonjour Bonjour Gateway related commands
 boot Display boot configuration.
 captive-portal Captive portal commands
 captive-portal-page-upload Captive portal internal and advanced page upload
```

|                           |                                             |
|---------------------------|---------------------------------------------|
| cdp                       | Cisco Discovery Protocol                    |
| classify-url              | Query the category of an URL                |
| clock                     | Display system clock                        |
| cluster                   | Cluster Protocol                            |
| cmp-factory-certs         | Display the CMP certificate status          |
| commands                  | Show command lists                          |
| context                   | Information about current context           |
| critical-resources        | Critical Resources                          |
| crypto                    | Encryption related commands                 |
| database                  | Database                                    |
| debug                     | Debugging functions                         |
| debugging                 | Debugging functions                         |
| device-upgrade            | Device Upgrade                              |
| dot1x                     | 802.1X                                      |
| dpi                       | Deep Packet Inspection                      |
| eguest                    | ExtremeGuest                                |
| environmental-sensor      | Display Environmental Sensor Module status  |
| event-history             | Display event history                       |
| event-system-policy       | Display event system policy                 |
| ex3500                    | EX3500 device details                       |
| extdev                    | External device (T5, Ex3500..)              |
| fabric-attach             | Fabric attach                               |
| file                      | Display filesystem information              |
| file-sync                 | File sync between controller and adoptees   |
| firewall                  | Wireless Firewall                           |
| global                    | Global-level information                    |
| gre                       | Show l2gre tunnel info                      |
| guest-notification-config | Show guest-notification information         |
| guest-registration        | Guest registration commands                 |
| interface                 | Interface Configuration/Statistics commands |
| ip                        | Internet Protocol (IP)                      |
| iot-device-type-imagotag  | Iot device type imagotag                    |
| ip-access-list            | IP ACL                                      |
| ipv6                      | Internet Protocol version 6 (IPv6)          |
| ipv6-access-list          | IPv6 ACL                                    |
| l2tpv3                    | L2TPv3 information                          |
| lACP                      | LACP commands                               |
| ldap-agent                | LDAP Agent Configuration                    |
| licenses                  | Show installed licenses and usage           |
| lldp                      | Link Layer Discovery Protocol               |
| logging                   | Show logging information                    |
| mac-access-list           | MAC ACL                                     |
| mac-address-table         | Display MAC address table                   |
| mac-auth                  | MAC authentication                          |
| mac-auth-clients          | MAC authenticated clients                   |
| mint                      | MiNT protocol                               |
| mirroring                 | Show mirroring sessions                     |
| nsight                    | Nsight Server Module                        |
| ntp                       | Network time protocol                       |
| password-encryption       | Password encryption                         |
| pppoe-client              | PPP Over Ethernet client                    |
| privilege                 | Show current privilege level                |
| radius                    | RADIUS statistics commands                  |
| raid                      | Show RAID status                            |
| reload                    | Scheduled reload information                |
| remote-debug              | Show details of remote debug sessions       |
| rf-domain-manager         | Show RF Domain Manager selection details    |
| role                      | Role based firewall                         |
| route-maps                | Display Route Map Statistics                |
| rtls                      | RTLS Statistics                             |
| running-config            | Current operating configuration             |
| session-changes           | Configuration changes made in this session  |
| session-config            | This session configuration                  |
| sessions                  | Display sessions                            |

```

site-config-diff Difference between site configuration on the NOC
 and actual site configuration
slot Expansion slots stats
smart-rf Smart-RF Management Commands
spanning-tree Display spanning tree information
startup-config Startup configuration
t5 Display T5 inventory information
terminal Display terminal configuration parameters
timezone The timezone
traffic-shape Display traffic shaping
upgrade-status Display last image upgrade status
version Display software & hardware version
virtual-machine Virtual Machine
vrrp VRRP protocol
web-filter Web filter
what Perform global search
wireless Wireless commands
wwan Display wireless WAN Status

```

```
<DEVICE>>
```

```
nx9500-6C8809#show wireless ap configured
```

| IDX | NAME          | MAC               | PROFILE        | RF-DOMAIN | ADOPTED-BY        |
|-----|---------------|-------------------|----------------|-----------|-------------------|
| 1   | ap7522-8330A4 | 84-24-8D-83-30-A4 | default-ap7522 | default   | 00-15-70-38-06-49 |
| 2   | ap8163-74B45C | B4-C7-99-74-B4-5C | default-ap81xx | default   | B4-C7-99-6D-B5-D4 |

```
nx9500-6C8809#
```

### adoption

Displays adoption related information, and is common to the User Exec, Priv Exec, and Global Config modes.

In an HM network devices are deployed in two levels. The first level consists of the NOC controllers. The second level consists of the site controllers that can be grouped to form clusters. The NOC controllers adopt and manage the site controllers. Access points within the network are adopted and managed by the site controllers. The adopted devices (access points and second-level controllers) are referred to as the adoptee. The devices adopting the adoptee are the 'adopters'.

Use this command to confirm if a device is an adoptee or an adopter. This command also allows you to determine the devices adopted by an adopter device.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```

show adoption [config-errors|controllers|history|info|log|offline|pending|status|timeline]
show adoption offline
show adoption config-errors <DEVICE-NAME>
show adoption log [adoptee|adopter {<MAC>}] {on <DEVICE-NAME>}
show adoption [controllers {include-ipv6}|history|info|pending|status {summary}|timeline]
{on <DEVICE-NAME>}

```

## Parameters

show adoption offline

|          |                                                                                 |
|----------|---------------------------------------------------------------------------------|
| adoption | Displays AP adoption history and status. It also displays configuration errors. |
| offline  | Displays non-adopted status of the logged device and its adopted Access Points  |

show adoption config-errors <DEVICE-NAME>

|                             |                                                                                                                                                                                                              |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| adoption                    | Displays AP adoption history and status. It also displays configuration errors.                                                                                                                              |
| config-errors <DEVICE-NAME> | Displays configuration errors for a specified adopted device <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

show adoption log [adoptee|adopter] {on <DEVICE-NAME>}

|                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| adoption                                                          | Displays adoption related information. It also displays configuration errors.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| log [adoptee adopter {MAC}] {on <DEVICE-NAME>} {on <DEVICE-NAME>} | <p>Displays adoption logs, for the specified device. If no device name is specified, the system displays logs for the logged device.</p> <ul style="list-style-type: none"> <li>• adoptee – Displays adoption logs for adoptee devices (APs, wireless controllers, and service platforms). To view logs for a specified adoptee, specify the device's name. If no device name is specified, the system displays logs for the logged device. If the logged device is not an adoptee, the system states that the device is a controller. for example, <pre>2013-01-19 22:00:13:MLCP_TAG_CLUSTER_MASTER not present and this device is a controller. Ignoring</pre> </li> <li>• on &lt;DEVICE-NAME&gt; – Optional. Displays adoptee status and details for the device identified by the &lt;DEVICE-NAME&gt; keyword <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; – Specify the device's name.</li> </ul> </li> <li>• adopter – Displays adoption logs for adopter devices (APs, wireless controllers, and service platforms). To view logs for a specified adopter, specify the device's name. If no device name is specified, the system displays logs for the logged device. <ul style="list-style-type: none"> <li>• &lt;MAC&gt; – Optional. Filters adopters by the adoptee device's MAC address. Specify the adoptee device's MAC address. The system displays logs for the device that has adopted the device identified by the &lt;MAC&gt; keyword. <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; – Optional. Displays adopter status and details for the device identified by the &lt;DEVICE-NAME&gt; keyword. Specify the adopter device's name. <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; – Specify the adopter device's name.</li> </ul> </li> </ul> </li> </ul> <p><b>Note:</b> A wireless controller or service platform cannot be configured as an adoptee and an adopter simultaneously. In other words, an adopted wireless controller or service platform cannot be configured to adopt another device and vice versa.</p> </li></ul> |

show adoption [history|controllers {include-ipv6}|info|pending|status {summary}|timeline] {on <DEVICE-NAME>}

|             |                                                                                                                                                                                                                                                                                                                    |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| adoption    | Displays AP adoption history and status. It also displays configuration errors.                                                                                                                                                                                                                                    |
| controllers | Displays information about adopted controllers. This is applicable in a Hierarchically managed network, where site controllers are adopted by the NOC controllers. <ul style="list-style-type: none"> <li>• include-ipv6 – Optional. Displays the controller's IPv6 address, if assigned, in the output</li> </ul> |

|                     |                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| history             | Displays the adoption history of the logged device and its adopted Access Points                                                                                                                                                                                                                                                                                      |
| info                | Displays adopted device information                                                                                                                                                                                                                                                                                                                                   |
| pending             | Displays information for devices pending adoption                                                                                                                                                                                                                                                                                                                     |
| status<br>{summary} | Displays adoption status for the logged device. When executed without using the 'on <DEVICE-NAME>' parameter, this command displays detailed information of all devices adopted by the device on which the command is executed. <ul style="list-style-type: none"> <li>summary - Optional. Displays a summary of all devices adopted by the logged device.</li> </ul> |
| timeline            | Displays the logged device's adoption timeline. It also shows the adoption time for the logged device's adopted APs. To view the adoption timeline of a specific device, use the on <DEVICE-NAME> option to specify the device.                                                                                                                                       |
| on <DEVICE-NAME>    | The following keywords are common to all of the above parameters: <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; - Optional. Displays a device's adoption information, based on the parameter passed.</li> <li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul>                                  |

### Usage Guidelines

In a device's Global Config mode, use the **customize > show-adoption-status** command to customize the **show > adoption > status** command output. The following columns can be added to the output:

```
nx9500-6C8809(config)#customize show-adoption-status ?
 adopted-by Device name to which the AP is adopted
 ap-name Host-name of the adopted AP
 cdp-lldp-info Cdp/lldp info of the Adopted AP
 config-status Configuration status of the adopted AP
 last-adoption Last known adoption time
 msgs Messages status
 uptime Uptime of the adopted AP
 version Current version of the adopted AP
nx9500-6C8809(config)#
```

For more information on the customize command, see [customize](#) on page 349.

### Examples

The following example displays details of the:

- device to which the logged device (rfs4000-6DB5D4) is adopted, and
- devices adopted by the logged device.

```
rfs4000-6DB5D4(config)#show adoption status
Adopted by:
Type : nx9000
System Name : nx9500-6C8809
MAC address : B4-C7-99-6C-88-09
MiNT address : 19.6C.88.09
Time : 7 days 01:02:34 ago

Adopted Devices:

DEVICE-NAME VERSION CFG-STAT MSGS ADOPTED-BY LAST-
ADOPTION UPTIME

ap8163-711728 5.9.2.0-012D configured No rfs4000-6DB5D4 0 days
23:42:11 0 days 23:46:12
```



```

ap7532-80C2AC 5.9.1.0-012D error Yes rfs4000-6DB5D4 1 days
00:10:00 1 days 00:11:40
ap8163-711634 5.9.2.0-012D configured No rfs4000-6DB5D4 1 days
00:23:12 1 days 02:13:48

```

-More--

```

rfs4000-6DB5D4(config)#
nx9500-6C8809#show adoption offline

```

```

MAC HOST-NAME TYPE RF-DOMAIN TIME OFFLINE
CONNECTED-TO

00-23-68-11-E6-C4 ap71xx-11E6C4 ap71xx TechPubs unknown
None
00-23-68-9C-63-D4 ap7161-9C63D4 ap71xx default unknown
None
84-24-8D-16-01-C4 ap7532-1601C4 ap7532 default unknown
None
B4-C7-99-4B-F3-64 ap7161-4BF364 ap71xx default unknown
None

```

Total number of devices displayed: 6

```

nx9500-6C8809#
nx9500-6C8809#show adoption log adoptee on default/ap7522-8330A4
2017-10-06 09:15:40:Received OK from cfgd, adoption complete to 70.38.06.49
2017-10-06 09:15:40:Waiting for cfgd OK, adopter should be 70.38.06.49
2017-10-06 09:15:40:Adoption state change: 'Connecting to adopter' to 'Waiting for
Adoption OK'
2017-10-06 09:15:40:Adoption state change: 'No adopters found' to 'Connecting to adopter'
2017-10-06 09:15:40:Try to adopt to 70.38.06.49 (cluster master 70.38.06.49 in adopters)
2017-10-06 09:15:38:Got new value for MTU: 1500 Was: 0
2017-10-06 09:15:38:MLCP created VLAN link on VLAN 1, offer from 00-15-70-38-06-49
2017-10-06 09:15:38:Sending MLCP Request to 00-15-70-38-06-49 vlan 1
2017-10-06 09:15:34:Received 0 hostnames through DHCP option 191
2017-10-06 09:15:34:Adoption state change: 'Disabled' to 'No adopters found'
2017-10-06 09:15:34:DNS resolution completed, starting MLCP
2017-10-06 09:15:34:Adoption enabled due to configuration
nx9500-6C8809#

```

## bluetooth

Displays Bluetooth radio statistics for RF Domain member access points

AP 8432 and AP 8533 model access points utilize a built-in Bluetooth chip for specific Bluetooth functional behaviors in a WiNG managed network. AP 8432 and AP 8533 models support both Bluetooth classic and BLE (Bluetooth low energy) technology. These platforms use their Bluetooth classic enabled radio to sense other Bluetooth enabled devices and report device data (MAC address, RSSI and device calls) to an ADSP server for intrusion detection. If the device presence varies in an unexpected manner, ADSP can raise an alarm.

AP 8432 and AP 8533 model access points support Bluetooth beaconing to emit either iBeacon or Eddystone-URL beacons. The access point's Bluetooth radio sends non-connectable, undirected LE (low-energy) advertisement packets periodically. These advertisement packets are short and sent on Bluetooth advertising channels that conform to already-established iBeacon and Eddystone-URL standards.

### Supported in the following platforms:

- Access Points — AP 8432, AP 8533

## Syntax

```
show bluetooth radio {detail/on}
show bluetooth radio {detail {<DEVICE-NAME> <1-1>/filter bluetooth-radio-mac <BT-RADIO-
MAC>}}
{(on <DEVICE-OR-DOMAIN-NAME>)}
```

## Parameters

```
show bluetooth radio {detail {<DEVICE-NAME> <1-1>/filter bluetooth-radio-mac <BT-RADIO-
MAC>}}
{(on <DEVICE-OR-DOMAIN-NAME>)}
```

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| bluetooth radio            | Displays Bluetooth radio utilization statistics based on the parameters passed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| detail <DEVICE-NAME> <1-1> | <p>Optional. Displays detailed Bluetooth radio utilization statistics. Optionally, to view detailed information for a specific access point's Bluetooth radio, specify the access point's and the radio's MAC addresses.</p> <ul style="list-style-type: none"><li>• &lt;DEVICE-NAME&gt; &lt;1-1&gt; - Optional. Specify the access point's hostname or MAC address.</li><li>• &lt;1-1&gt; - Specify the bluetooth radio interface index number from 1 - 1. As of now only one Bluetooth radio interface is supported. The Interface index number is appended to the AP's hostname or MAC address in the following format: ap8533-06FBE1:B1 OR 74-67-F7-06-FB-E1:B1</li></ul> <p>The following information is displayed:</p> <ul style="list-style-type: none"><li>• access point's hostname as its network identifier</li><li>• access point's alias. If an alias has been defined for the access point it is listed here. The alias value is expressed in the form of &lt;hostname&gt;:B&lt;Bluetooth_radio_number&gt;. If the access point has a administrator assigned hostname, it is used in place of the access point's default hostname.</li><li>• access point's factory encoded MAC address</li><li>• access point and bluetooth radio's administrator assigned area of deployment (the AP's geographical location)</li><li>• bluetooth radio's state (on/off)</li><li>• bluetooth radio's reason for inactivity (in case the radio is off)</li><li>• bluetooth radio's factory encoded MAC address serving as this device's hardware identifier on the network</li><li>• bluetooth radio's functional mode: bt-sensor or le-beacon</li><li>• bluetooth radio's beacon period</li><li>• bluetooth radio's beacon type</li><li>• descriptive text on any error that's preventing the Bluetooth radio from operating</li></ul> |

|                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| filter bluetooth-radio-mac <BT-RADIO-MAC> | Optional. Specifies additional filters to get table values. Filters data based on the Bluetooth radio's MAC address. <ul style="list-style-type: none"> <li>&lt;BT-RADIO-MAC&gt; - Specify the Bluetooth radio's MAC address. The system only displays statistics related to the specified Bluetooth radio.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| on <DEVICE-OR-DOMAIN-NAME>                | The following keywords are recursive and common to all of the above. <ul style="list-style-type: none"> <li>on &lt;DEVICE-OR-DOMAIN-NAME&gt; - Optional. Displays Bluetooth radio statistics on a specified device or RF Domain <ul style="list-style-type: none"> <li>&lt;DEVICE-OR-DOMAIN-NAME&gt; - Specify the name of the device or RF Domain. If the device name is explicitly given, the results display data for the specified AP only. If the RF Domain is explicitly given, the results display data for all APs within the specified RF Domain.</li> </ul> </li> </ul> <p>If no device/RF Domain is specified, the results include data for all Bluetooth radios within the controller's RF Domain.<br/>If the controller is in the "on rf-domain all" mode, the results include data for all Bluetooth radios for all APs in each domain known to the controller.</p> |

### Examples

```
nx9500-6C8809(config)#show bluetooth radio on ap8533-06F808
```

```

BLUETOOTH RADIO RADIO MAC MODES STATE

ap8533-06F808:B1 74-67-F7-08-A3-B0 BLE-Beacon On

```

```
Total number of Bluetooth radios displayed: 0
```

```
nx9500-6C8809(config)#
```

```
nx9500-6C8809(config)#show bluetooth radio detail 74-67-F7-06-F8-08 1
```

```
Radio: 74-67-F7-06-F8-08:B1, alias ap8533-06F808:B1
```

```
STATE : Off [shutdown in cfg]
PHY INFO : MAC: 74-67-F7-08-A3-B0
ACCESS POINT : Name: ap8533-06F808 Location: default Placement: Indoor
ENABLED MODES : BLE-Beacon
BEACON TYPES : Eddystone-URL
BEACON PERIOD : 1000ms
Last error :
```

```
nx9500-6C8809(config)#
```

### boot

Displays a device's boot configuration. Use this command to view the primary and secondary image details, such as Build Date, Install Date, and Version. This command also displays the current boot and next boot information.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show boot {on <DEVICE-NAME>}
```

### Parameters

```
show boot {on <DEVICE-NAME>}
```

|                  |                                                                                                                                                                                                                                                                                                                         |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| boot             | Displays primary and secondary image boot configuration details (build date, install date, version, and the image used to boot the current session)                                                                                                                                                                     |
| on <DEVICE-NAME> | Optional. Displays a specified device's boot configuration <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> <p><b>Note:</b> Use the <i>on</i> &lt;DEVICE-NAME&gt; option to view a remote device's boot configuration.</p> |

### Examples

```
NOC-NX9500#show boot
```

```

 IMAGE BUILD DATE INSTALL DATE VERSION

 Primary 09/21/2017 14:51:03 09/22/2017 10:32:33 5.9.1.0-029R
 Secondary 12/14/2017 13:57:13 01/03/2018 10:33:25 5.9.2.0-005D

Current Boot : Primary
Next Boot : Secondary
Software Fallback : Enabled
VM support : Not present
NOC-NX9500#
```

### bonjour

Displays the configured Bonjour services available on local and remote sites

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show bonjour services {on <DEVICE-NAME>}
```

### Parameters

```
show bonjour services {on <DEVICE-NAME>}
```

|                  |                                                                                                                                                                                                                   |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| bonjour services | Displays the configured Bonjour services available on local and remote sites                                                                                                                                      |
| on <DEVICE-NAME> | Optional. Displays Bonjour services available on a specified device <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

### Examples

```
nx9500-6C8809#show bonjour services onap7161-11E6C4
```

```

 SERVICE_NAME INSTANCE_NAME
 IP:PORT VLAN-ID VLAN_TYPE EXPIRY

 _pdl-datastream._tcp.local Brother MFC-8510DN._pdl-datastream._tcp.local
 172.110.0.146:9100 110 Local Tue Sep 12 02:07:44 2017

```

```

_universal._sub._ipp._tcp.local Brother MFC-8510DN._ipp._tcp.local
172.110.0.146:631 110 Local Tue Sep 12 02:36:13 2017

_ipp._tcp.local Brother MFC-8510DN._ipp._tcp.local
172.110.0.146:631 110 Local Tue Sep 12 02:36:13 2017

nx9500-6C88099#

```

### *captive-portal*

Displays WLAN captive portal information. Use this command to view a configured captive portal's client information.

#### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### **Syntax**

```

show captive-portal sessions {include-ipv6/on <DEVICE-OR-DOMAIN-NAME>/statistics}
{(filter [captive-portal [<CAPTIVE-PORTAL>/not <CAPTIVE-PORTAL>]|ip [<IPv4>/not <IPv4>]|
ipv6 [<IPv6>/not <IPv6>]|state [pending/success/not [pending/success]]|vlan [<VLAN-ID>/
not <VLAN-ID>]|wlan [<WLAN-NAME>/not <WLAN-NAME>]})}

```

#### **Parameters**

```

show captive-portal sessions {include-ipv6/on <DEVICE-OR-DOMAIN-NAME>/statistics}
{(filter [captive-portal [<CAPTIVE-PORTAL>/not <CAPTIVE-PORTAL>]|ip [<IPv4>/not <IPv4>]|
ipv6 [<IPv6>/not <IPv6>]|state [pending/success/not [pending/success]]|vlan [<VLAN-ID>/
not <VLAN-ID>]|wlan [<WLAN-NAME>/not <WLAN-NAME>]})}

```

|                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| captive-portal sessions                                | Displays active captive portal client session details                                                                                                                                                                                                                                                                                                                                                                                                  |
| include-ipv6                                           | Optional. Includes IPv6 address (if known) of captive portal clients. By default the system only displays IPv4 addresses. The include-ipv6 parameter includes IPv6 address (if known) of each client.                                                                                                                                                                                                                                                  |
| statistics                                             | Optional. Displays statistical information regarding client sessions                                                                                                                                                                                                                                                                                                                                                                                   |
| on <DEVICE-OR-DOMAIN-NAME>                             | Optional. Displays active captive portal session details on a specified device or RF Domain. <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; - Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul>                                                                                                                                                                                      |
| filter                                                 | This parameter is recursive and can be used with any of the above parameters to define additional filters.<br>Optional. Defines additional filters. Use one of the following options: <b>captive-portal</b> , <b>ip</b> , <b>ipv6</b> , <b>state</b> , <b>vlan</b> , or <b>wlan</b> .                                                                                                                                                                  |
| captive-portal [<CAPTIVE-PORTAL>] not <CAPTIVE-PORTAL> | Optional. Displays captive portal client and client session information, based on the captive portal name passed <ul style="list-style-type: none"> <li>• &lt;CAPTIVE-PORTAL&gt; - Specify the captive portal name. Displays client details for the specified captive portal.</li> <li>• not &lt;CAPTIVE-PORTAL&gt; - Inverts the match selection. Displays client details for all captive portals other than the specified captive portal.</li> </ul> |

|                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip [<IPv4> not <IPv4>]                         | Optional. Displays captive portal client/client sessions information, based on the IPv4 address passed <ul style="list-style-type: none"> <li>• &lt;IPv4&gt; - Specify the client's IPv4 address. Displays information of the client identified by the &lt;IPv4&gt; parameter.</li> <li>• not &lt;IPv4&gt; - Inverts the match selection. Displays client details for all clients other than the one identified by the &lt;IPv4&gt; parameter.</li> </ul>                                                                                                                                                                                             |
| ipv6 [<IPv6> not <IPv6>]                       | This filter option is available only for the 'include-ipv6' keyword.<br>Optional. Displays captive portal client/client sessions information, based on the IPv6 address passed <ul style="list-style-type: none"> <li>• &lt;IPv6&gt; - Specify the client's IPv6 address. Displays information of the client identified by the &lt;IPv6&gt; parameter</li> <li>• not &lt;IPv6&gt; - Inverts the match selection. Displays client details for all clients other than the one identified by the &lt;IPv6&gt; parameter.</li> </ul>                                                                                                                      |
| state [pending success  not [pending success]] | Optional. Filters clients/client sessions based on the client's authentication state <ul style="list-style-type: none"> <li>• pending - Displays information of clients redirected for authentication</li> <li>• success - Displays information of successfully authenticated clients</li> <li>• not [pending success] - Inverts match selection <ul style="list-style-type: none"> <li>• pending - Displays information of successfully authenticated clients (opposite of pending authentication)</li> <li>• success - Displays information of clients redirected for authentication (opposite of successful authentication)</li> </ul> </li> </ul> |
| vlan [<VLAN-ID> not <VLAN-ID>]                 | Optional. Displays captive portal client/client sessions information based on the VLAN ID passed <ul style="list-style-type: none"> <li>• &lt;VLAN-ID&gt; - Specify the VLAN ID. Displays client details for the specified VLAN.</li> <li>• not &lt;VLAN-ID&gt; - Inverts match selection. Displays client details for all VLANs other than the one identified by the &lt;VLAN-ID&gt; parameter.</li> </ul>                                                                                                                                                                                                                                           |
| wlan [<WLAN-NAME> not <WLAN-NAME>]             | Optional. Displays captive portal client/client sessions information based on the WLAN name passed <ul style="list-style-type: none"> <li>• &lt;WLAN-NAME&gt; - Specify the WLAN name. Displays client details for the specified WLAN.</li> <li>• not &lt;WLAN-NAME&gt; - Inverts match selection. Displays client details for all WLANs other than the one identified by the &lt;WLAN-NAME&gt; parameter.</li> </ul>                                                                                                                                                                                                                                 |

### Examples

```
rfs4000-229D58#show captive-portal sessions
=====
CLIENT IPv4 CAPTIVE-PORTAL WLAN/PORT VLAN STATE SESSION TIME

00-26-55-F4-5F-79 192.168.3.99 cappo rfs4000-229D58:ge2 400 Success
23:58:35
=====
Total number of captive portal sessions displayed: 1
rfs4000-229D58#
```

### *captive-portal-page-upload (show commands)*

Displays captive portal page information, such as upload history, upload status, and page file download status

## Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
show captive-portal-page-upload [history|list-files|load-image-status|status]
show captive-portal-page-upload load-image-status
show captive-portal-page-upload history {on <RF-DOMAIN-NAME>}
show captive-portal-page-upload status {on [<RF-DOMAIN-NAME>/<RF-DOMAIN-MANAGER>]}
show captive-portal-page-upload list-files <CAPTIVE-PORTAL-NAME>
```

## Parameters

```
show captive-portal-page-upload load-image-status
```

|                   |                                                                               |
|-------------------|-------------------------------------------------------------------------------|
| load-image-status | Displays captive portal advanced page file upload status on the logged device |
|-------------------|-------------------------------------------------------------------------------|

```
show captive-portal-page-upload history {on <RF-DOMAIN-NAME>}
```

|                               |                                                                                                                                                                                                                                           |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| history {on <RF-DOMAIN-NAME>} | Displays captive portal page upload history <ul style="list-style-type: none"><li>• on &lt;RF-DOMAIN-NAME&gt; - Optional. Displays captive portal page upload history within a specified RF Domain. Specify the RF Domain name.</li></ul> |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
show captive-portal-page-upload status {on [<RF-DOMAIN-NAME>/<RF-DOMAIN-MANAGER>]}
```

|                                                    |                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| status {on [<RF-DOMAIN-NAME>/<RF-DOMAIN-MANAGER>]} | Displays captive portal page upload status <ul style="list-style-type: none"><li>• on &lt;RF-DOMAIN-NAME&gt; - Optional. Displays captive portal page upload status within a specified RF Domain. Specify the RF Domain name.</li><li>• on &lt;RF-DOMAIN-MANAGER&gt; - Optional. Displays captive portal page upload status for a specified RF Domain Manager. Specify the RF Domain Manager name.</li></ul> |
|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
show captive-portal-page-upload list-files <CAPTIVE-PORTAL-NAME>
```

|                                  |                                                                                                                                                                                                                                                   |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| list-files <CAPTIVE-PORTAL-NAME> | Displays a list of all captive portal Web page files, of a specified captive portal, uploaded (internal and advanced page files) <ul style="list-style-type: none"><li>• &lt;CAPTIVE-PORTAL-NAME&gt; - Specify the captive portal name.</li></ul> |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx7500-7F2C13#show captive-portal-page-upload CP-BW all
```

```

 CONTROLLER STATUS MESSAGE

 84-24-8D-7F-2C-13 Success Added 1 APs to upload queue

```

```
nx7500-7F2C13#
nx7500-7F2C13#show captive-portal-page-upload load-file-status
Download of CP-BW page file is complete
nx7500-7F2C13#
```

```
nx7500-7F2C13#show captive-portal-page-upload list-files CP-BW
```

```

 NAME SIZE LAST MODIFIED

```

```

CP-BW-1.tar.gz 6133 2016-05-16 10:38:40
CP-BW.tar.gz 3370 2016-05-16 10:45:44

nx7500-7F2C13#
<exsw1>show captive-portal-page-upload load-image-status
No captive portal advanced page file download is in progress
<exsw1>

```

## cdp

Displays the CDP neighbor table

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show cdp [neighbors|report] {detail {on <DEVICE-NAME>}/on <DEVICE-NAME>}
```

### Parameters

```
show cdp [neighbors|report] {detail {on <DEVICE-NAME>}/on <DEVICE-NAME>}
```

|                           |                                                                                                                                                                                                                                                                                                                              |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cdp [neighbors report]    | Displays CDP neighbors table or aggregated CDP neighbors table                                                                                                                                                                                                                                                               |
| detail {on <DEVICE-NAME>} | Optional. Displays detailed CDP neighbors table or aggregated CDP neighbors table <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; - Optional. Displays table details on a specified device</li> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |
| on <DEVICE-NAME>          | Optional. Displays table details on a specified device <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul>                                                                                                                       |

### Examples

The following example shows detailed CDP neighbors table:

```

nx9500-6C8809#show cdp neighbors detail

Device ID: ap8163-74B45C
Entry address(es):
 IP Address: 192.168.13.26
Platform: AP-8163-66040-WR, Capabilities: Router Switch
Interface: ge1, Port ID (outgoing port): ge1
Hold Time: 165 sec

advertisement version: 2
Native VLAN: 1
Duplex: full
Version :
5.9.2.0-007D

Device ID: ap7532-80C2AC
Entry address(es):
 IP Address: 192.168.13.28

```



```
Platform: AP-7532-67040-WR, Capabilities: Router Switch
Interface: ge1, Port ID (outgoing port): ge1
Hold Time: 169 sec
```

```
--More--
nx9500-6C8809#
```

The following example shows a non-detailed CDP neighbors table:

```
nx9500-6C8809#show cdp neighbors

 Device ID Platform Local Interface Port ID Duplex

 rfs4000-880DA7 RFS-4010-11110-US ge2 ge1 full

nx9500-6C8809#
```

### *classify-url*

Displays a specified URL's category. Use this command to query the category of a specific URL. The query is sent to a configured classification server. This option is available only if a valid URL filter license is available.

#### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### **Syntax**

```
show classify-url [<URL-TO-QUERY>|datacenter <URL-TO-QUERY>]
```

#### **Parameters**

```
show classify-url [<URL-TO-QUERY>|datacenter <URL-TO-QUERY>]
```

|                           |                                                                                                                                                            |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| classify-url              | Queries the category of a specified URL                                                                                                                    |
| <URL-TO-QUERY>            | Specify the URL to query. The query is sent to the configured classification server.                                                                       |
| datacenter <URL-TO-QUERY> | The query is sent to a global classification datacenter <ul style="list-style-type: none"><li>• &lt;URL-TO-QUERY&gt; - Specify the URL to query.</li></ul> |

#### **Examples**

```
nx9500-6C8809#show classify-url www.google.com
Categories: search-engines-portals,
Custom Categories:
nx9500-6C8809#
nx9500-6C8809#show classify-url www.ndtv.com
Categories: news,
Custom Categories: list1,
nx9500-6C8809#
```

### *clock*

Displays system clock on the logged device or on a specified device

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show clock {on <DEVICE-NAME>}
```

### Parameters

```
show clock {on <DEVICE-NAME>}
```

|                  |                                                                                                                                                                                                                |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| clock            | Displays a system's clock                                                                                                                                                                                      |
| on <DEVICE-NAME> | Optional. Displays system clock on a specified device <ul style="list-style-type: none"><li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, service platform, or RF Domain.</li></ul> |

### Examples

```
ap8432-070235>show clock
2018-01-09 02:34:22 UTC
ap8432-070235>
```

## cluster

Displays cluster information (cluster configuration parameters, members, status, etc.)

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show cluster [configuration|history|members|status]
show cluster [configuration|history {on <DEVICE-NAME>}|members {detail}|status]
```

### Parameters

```
show cluster [configuration|history {on <DEVICE-NAME>}|members {detail}|status]
```

|                          |                                                                                                                                                                                                                                              |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cluster                  | Displays cluster information                                                                                                                                                                                                                 |
| configuration            | Displays cluster configuration details                                                                                                                                                                                                       |
| history on <DEVICE-NAME> | Displays cluster history status <ul style="list-style-type: none"><li>• &lt;DEVICE-NAME&gt; - Optional. Specify the controller or access point name. If the device name is not specified, the system displays all cluster history.</li></ul> |
| members {detail}         | Displays cluster members configured on the logged device <ul style="list-style-type: none"><li>• detail - Optional. Displays detailed information of known cluster members</li></ul>                                                         |
| status                   | Displays cluster status                                                                                                                                                                                                                      |

## Examples

```
nx9500-6C8809(config)#show cluster configuration
Cluster Configuration Information
```

```
Name : SiteConRFS6k
Configured Mode : Active
Master Priority : 128
Force configured state : Disabled
Force configured state delay : 5 minutes
Handle STP : Disabled
Radius Counter DB Sync Time : 5 minutes
```

```
nx9500-6C8809(config)#
```

```
nx9500-6C8809(config)#show cluster members detail
```

```

 ID MAC MODE AP COUNT AAP COUNT AP LICENSE AAP LICENSE
VERSION

70.38.06.49 00-15-70-38-06-49 Active 0 1 0 0
5.9.2.0-007D
70.81.74.2D 00-15-70-81-74-2D Active 0 0 1 0
9.2.0-007D

```

```
nx9500-6C8809(config)#
```

```
nx9500-6C8809(config)#show cluster status
```

```
Cluster Runtime Information
```

```
Protocol version : 1
Cluster operational state : active
AP license : 0
AAP license : 0
AP count : 0
AAP count : 0
Max AP adoption capacity : 1024
Number of connected member(s) : 0
```

```
nx9500-6C8809(config)#
```

## *cmp-factory-certs*

Displays factory installed CMP certificates

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show cmp-factory-certs {all}
```

### Parameters

```
show cmp-factory-certs {all}
```

|                         |                                                                                                                                 |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| cmp-factory-certs {all} | Displays factory installed CMP certificates on the logged device. Optionally use the 'all' keyword to view certificate details. |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809>show cmp-factory-certs
No CMP factory certificate exist
nx9500-6C8809>
```

---

## commands

Displays commands available for the current mode

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show commands
```

### Parameters

None

### Examples

```
rfs4000-880DA7(config)#show commands
 help
 help search WORD (|detailed|only-show|skip-show|skip-no)
 show commands
 show adoption log adoptee(|on DEVICE-NAME)
 show adoption log adopter (|mac AA-BB-CC-DD-EE-FF)(|on DEVICE-NAME)
 show adoption info (|on DEVICE-NAME)
 show adoption status (|on DEVICE-NAME)
 show adoption status summary (|on DEVICE-NAME)
 show adoption config-errors DEVICE-NAME
 show adoption offline
 show adoption pending (|on DEVICE-NAME)
 show adoption history (|on DEVICE-NAME)
 show adoption timeline (|on DEVICE-NAME)
 show adoption controllers (|on DEVICE-NAME)
 show adoption controllers include-ipv6(|on DEVICE-NAME)
 show debugging (|on DEVICE-OR-DOMAIN-NAME)
 show debugging cfgd(|on DEVICE-NAME)
 show debugging fib(|on DEVICE-NAME)
 show debugging adoption (|on DEVICE-OR-DOMAIN-NAME)
 show debugging wireless (|on DEVICE-OR-DOMAIN-NAME)
 show debugging snmp (|on DEVICE-NAME)
 show debugging ssm (|on DEVICE-NAME)
 show debugging voice (|on DEVICE-OR-DOMAIN-NAME)
--More--
rfs4000-880DA7(config)#
```

## context

Displays the current context details

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
show context {include-factory/session-config {include-factory}}
```

## Parameters

```
show context {include-factory/session-config {include-factory}}
```

|                                |                                                                                                                                                                            |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| include-factory                | Optional. Includes factory defaults                                                                                                                                        |
| session-config include-factory | Optional. Displays running system information in the current context <ul style="list-style-type: none"><li>include-factory – Optional. Includes factory defaults</li></ul> |

## Examples

```
ap8432-070235>show context
!
! Configuration of AP8432 version 5.9.2.0-008D
!
!
version 2.5
!
!
client-identity-group default
 load default-fingerprints
!
ip access-list BROADCAST-MULTICAST-CONTROL
 permit tcp any any rule-precedence 10 rule-description "permit all TCP traffic"
 permit udp any eq 67 any eq dhcpc rule-precedence 11 rule-description "permit DHCP
replies"
 deny udp any range 137 138 any range 137 138 rule-precedence 20 rule-description "deny
windows netbios"
 deny ip any 224.0.0.0/4 rule-precedence 21 rule-description "deny IP multicast"
 deny ip any host 255.255.255.255 rule-precedence 22 rule-description "deny IP local
broadcast"
 permit ip any any rule-precedence 100 rule-description "permit all IP traffic"
!
--More--
ap8432-070235>
```

## *critical-resources*

Displays critical resource information. Critical resources are resources vital to the network.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
show critical-resources {on <DEVICE-NAME>}
```

## Parameters

```
show critical-resources {on <DEVICE-NAME>}
```

|                    |                                                                                                                                                                                                                      |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| critical-resources | Displays critical resources information                                                                                                                                                                              |
| on <DEVICE-NAME>   | Optional. Displays critical resource information on a specified device <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

### Examples

```
rfs4000-229D58(config)#show critical-resources

CRITICAL RESOURCE IP VLAN PING-MODE STATE

172.168.1.103 1 arp-icmp up

rfs4000-229D58(config)#
```

### crypto

Displays encryption mode information

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show crypto [cmp|ike|ipsec|key|pki]
show crypto cmp request status
show crypto ike sa {detail/on/peer/version}
show crypto ike sa {detail/peer <IP>} {on <DEVICE-NAME>}
show crypto ike sa {version [1/2]} {peer <IP>} {(on <DEVICE-NAME>)}
show crypto ipsec sa {detail/on/peer}
show crypto ipsec sa {detail} {on <DEVICE-NAME>}
show crypto ipsec sa {peer <IP>} {detail} {(on <DEVICE-NAME>)}
show crypto key rsa {on/public-key-detail}
show crypto key rsa {public-key-detail} {(on <DEVICE-NAME>)}
show crypto pki trustpoints {<TRUSTPOINT-NAME>|all/on}
show crypto pki trustpoints {<TRUSTPOINT-NAME>|all} {(on <DEVICE-NAME>)}
```

### Parameters

show crypto cmp request status

|                    |                                                                                       |
|--------------------|---------------------------------------------------------------------------------------|
| crypto cmp request | Displays current status of in-progress CMP (certificate management protocol) requests |
| status             | For more information, see <a href="#">CRYPTO-CMP-POLICY</a> .                         |

```
show crypto ike sa {detail/peer <IP>} {on <DEVICE-NAME>}
```

|               |                                                                           |
|---------------|---------------------------------------------------------------------------|
| crypto ike sa | Displays IKE (Internet Key Exchange) SA (security association) statistics |
| detail        | Displays detailed IKE SA statistics                                       |

|                  |                                                                                                                                                                                                            |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| peer <IP>        | Optional. Displays IKE SA statistics for a specified peer <ul style="list-style-type: none"> <li>• &lt;IP&gt; – Specify the peer’s IP address in the A.B.C.D format</li> </ul>                             |
| on <DEVICE-NAME> | Optional. Displays IKE SA statistics on a specified device <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
show crypto ike sa {version [1|2]} {peer <IP>} {(on <DEVICE-NAME>)}
```

|                  |                                                                                                                                                                                                    |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| crypto ike sa    | Displays IKE SA details                                                                                                                                                                            |
| version [1 2]    | Optional. Displays IKE SA version statistics <ul style="list-style-type: none"> <li>• 1 – Displays IKEv1 statistics</li> <li>• 2 – Displays IKEv2 statistics</li> </ul>                            |
| on <DEVICE-NAME> | Optional. Displays IPSec SAs on a specified device <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
show crypto sa {peer <IP>} {detail} {(on <DEVICE-NAME>)}
```

|                  |                                                                                                                                                                                                                                                                            |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| crypto ipsec sa  | Displays IPSec SA statistics. The IPSec encryption authenticates and encrypts each IP packet in a communication session                                                                                                                                                    |
| peer <IP> detail | Optional. Displays IPSec SA statistics for a specified peer <ul style="list-style-type: none"> <li>• &lt;IP&gt; – Specify the peer’s IP address in the A.B.C.D format.</li> <li>• detail – Displays detailed IPSec SA statistics for the specified peer</li> </ul>         |
| on <DEVICE-NAME> | The following keyword is recursive: <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; – Optional. Displays IPSec SAs on a specified device</li> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
show crypto key rsa {public-key-detail} {(on <DEVICE-NAME>)}
```

|                   |                                                                                                                                                                                                                                                                             |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| crypto key rsa    | Displays RSA public keys                                                                                                                                                                                                                                                    |
| public-key-detail | Optional. Displays public key in the PEM ( <i>Privacy-Enhanced Mail</i> ) format                                                                                                                                                                                            |
| on <DEVICE-NAME>  | The following keyword is recursive: <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; – Optional. Displays public key on a specified device</li> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
show crypto pki trustpoints {<TRUSTPOINT-NAME>|all} {(on <DEVICE-NAME>)}
```

|                   |                                                                                                         |
|-------------------|---------------------------------------------------------------------------------------------------------|
| crypto pki        | Displays PKI related information                                                                        |
| trustpoints       | Displays WLAN trustpoints<br>This command displays all trustpoints including CMP-generated trustpoints. |
| <TRUSTPOINT-NAME> | Optional. Displays a specified trustpoint details. Specify the trustpoint name.                         |

|                  |                                                                                                                                                                                                                                                                                                                                              |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| all              | Optional. Displays details of all trustpoints                                                                                                                                                                                                                                                                                                |
| on <DEVICE-NAME> | The following keyword is recursive and common to the 'trustpoint-name' and 'all' parameters: <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; - Optional. Displays trustpoints configured on a specified device</li> <li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

## Examples

```
nx9500-6C8809(config)#show crypto key rsa public-key-detail
```

```
RSA key name: ting Key-length: 2048
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtLj1lyR38+/mcInGRlrw
3DaasuTJhKsWg7kcSVkM7RLd/Wq/mPZEsqwFLnvFIm4rVIke+mVdWBqV4oGE1TUm
Z4YqKtzlANSAG7EZREr3MXEIHd49NHYeK8U+1EAmHN9F21XCxTO+yRMngKDJeHfz
Za2/64PdBsnRlV4nqCGMGHbbaaCwGe5X0a
```

```
RSA key name: default_rsa_key Key-length: 2048
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAE3hyJDk9aMk97X3PhoyMb
6nufFLFuKpF9YwSqO2fNyp9SutqpoML/VAMHHotmaa6SsxPURF8mC66bT7De32r7
wwPd7pIWwALTscwCzd3CrBljY8s2OQ7ZHGCH6MLau+LeonPE0c+uH3tNLloTAvSG
xtUAHfwFa4rM6vlzs/ejJ4InnboI8i4uIA
```

```
nx9500-6C8809(config)#
nx9500-6C8809(config)#show crypto key rsa
```

```

KEY NAME KEY LENGTH

1 ting 2048
2 default_rsa_key 2048

```

```
nx9500-6C8809(config)#
```

```
nx9500-6C8809(config)#show crypto pki trustpoints all
```

```
Trustpoint Name: default-trustpoint (self signed)
```

```

CRL present: no
Server Certificate details:
 Key used: default_rsa_key
 Serial Number: 051d
 Subject Name:
 /CN=NX9500-B4-C7-99-6C-88-09
 Issuer Name:
 /CN=NX9500-B4-C7-99-6C-88-09
 Valid From : Thu Dec 5 04:15:59 2013 UTC
 Valid Until: Sun Dec 3 04:15:59 2023 UTC
```

```
nx9500-6C8809(config)#
nx9500-6C8809>show crypto cmp request status
CMP Request Status: ir-req-reset
nx9500-6C8809>
```

## database

Displays database-related statistics and status



## Supported in the following platforms:

- Service Platforms — NX 95XX, VX 9000

## Syntax

```
show database [backup-status|keyfile|restore-status|statistics|status|users] {on <DEVICE-NAME>}
```

## Parameters

```
show database [backup-status|keyfile|restore-status|statistics|status|users] {on <DEVICE-NAME>}
```

|                  |                                                                                                                                                                                                                     |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| database         | Displays all configured database-related statistics and status                                                                                                                                                      |
| backup-status    | Displays the last database backup status                                                                                                                                                                            |
| keyfile          | Displays the keyfiles generated on the database host to enable authenticated database access                                                                                                                        |
| back-restore     | Displays the last database restore status                                                                                                                                                                           |
| statistics       | Displays database-related statistics, such as name of the database (NSight or captive portal), data size, storage size, free disk space available, etc.                                                             |
| status           | Displays database status, such as online time.                                                                                                                                                                      |
| users            | Displays database users created. These are the users that can access the databases.                                                                                                                                 |
| on <DEVICE-NAME> | Optional. Displays database-related information on a specified device <ul style="list-style-type: none"><li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li></ul> |

## Examples

```
vx9000-D031F2(config)#show database backup-status detail
Last Database Backup Status : Failed(Error in ftp: 1)
Last Database Backup Time : 2017-04-11 08:03:10

Starting backup of mart ...
connected to: 127.0.0.1
2015-05-20T14:02:46.340+0530 DATABASE: mart to dump/mart
2015-05-20T14:02:46.341+0530 mart.system.indexes to dump/mart/system.indexes.bson
2015-05-20T14:02:46.341+0530 61 documents
2015-05-20T14:02:46.341+0530 mart.wlan_info to dump/mart/wlan_info.bson
2015-05-20T14:02:46.341+0530 5 documents
2015-05-20T14:02:46.342+0530 Metadata for mart.wlan_info to dump/mart/
2015-05-20T14:02:46.342+0530 wlan_info.metadata.json
2015-05-20T14:02:46.342+0530 mart.rf_domain_info to dump/mart/rf_domain_info.bson
2015-05-20T14:02:46.342+0530 21 documents
2015-05-20T14:02:46.342+0530 Metadata for mart.rf_domain_info to dump/mart/
2015-05-20T14:02:46.342+0530 rf_domain_info.metadata.json
--More--
vx9000-D031F2(config)#
vx9000-D031F2(config)#show database status

MEMBER STATE ONLINE TIME

localhost PRIMARY 2 days 3 hours 45 min 24 sec

Authentication: Disabled Authentication User: None

```

```
[*] indicates this device.
vx9000-D031F2(config)#
vx9000-D031F2(config)#show database statistics
```

| DATABASE       | STORAGE SIZE | DATA SIZE | INDEX SIZE | DISK FREE |
|----------------|--------------|-----------|------------|-----------|
| admin          | 32k          | 335       | 48k        | 594.5G    |
| captive-portal | 4k           | 0         | 24k        | 594.5G    |
| nsightcache    | 96k          | 2.0k      | 264k       | 594.5G    |
| nsight         | 26.1M        | 136.6M    | 18.9M      | 594.5G    |

```
vx9000-D031F2(config)#
nx9500-6C8809#show database keyfile
```

```
SLz6lVXyi9vyTCChUKs04THRo3mWojZheM58Dt6NC0MDkdGv+5+wWN9/IT6zfy1s
KPut4BPpUWym8MEaRmapg4kRrN/SMSMlH6sPITMGTLmu6wRYFEUgKg001Wn/BohE
5n+uuhY0xiZQsN0LS7IaA8Yb9rX859YRQ7v9By5aEpi1NIDR4KX09Xs3TqIB+5v2
jE3vv70sKK+LX63bcIoYo35MX251T2pHdL+fMdLfkPMT8ZbzYzx2b22Yvukfg0gm
xHsMCB+bLAsfkjeCPgHCAq/WWi3Kxna6ysFjp8J4US2Bm+GL1COvALbCQBwkPPN+
o7M90qt40AubibBkeID2S9rkQkKcXqGESbL5xG6ip+26jIxiLv7GP6/SQZGF0qC/
ZZEkCNhGhkiykti0IxBfoXwoy66sqQ4KBwLF449eqBe7Svel/dzppFPNFYzpw8SMY
LD6iLTPR9BddjsBBEj8kGGc5R+M0R6lgQFEew2WX6Rqz45YTGecfOk18c9wl3taD
xn4imhI/esjMppFDu5muxRHF5RHa5RncTGnsMfc7ndvU178QaGHLZvDqjNLBUUnuP
c8QmyohEnKf70TYx/ruG9Vb2AP0Jw500DTNh2lmaoFjicKYQr+xIHUJpHc0qY43C
5Wz1Wf84CK67cu7kOPiJoaxvufzSXhJB18BiCXtUv40+ZZ6e3PcisZuIrPXxCZup
GJ3KpuHq61IjyVCydfD5z14Fho+RGAQ9d1DIlaLjbW+YT4CEH1bTiUmreUt+D/X2
zcB9nec77wIIAcdf12qysgGIqmKI3jRI89d3XM5Y7Kc2TuXBVZOazYldPj+qE/yi
EgVWcbtvvyS834jit35MGbVXhvQ2d45qgo42WZwdTVLXC9memzoKa3YIZoj32uP3U
iOrzd8E1gMte4gDE/KmGkYya+hsWswBmKClv0gj5NQ6TejYS4z+nefqLHUSVXbQ8
NxRel1huGi8P1ns4dWCwClWp8GpxUTa7GuN1DySA7/12OJM=
```

```
nx9500-6C8809#
```

## Related Commands

|  |
|--|
|  |
|--|

### device-upgrade

Displays firmware upgradation information for devices adopted by a wireless controller or access point

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
show device-upgrade [history|load-image-status|status|versions]
show device-upgrade [history {on <DOMAIN-NAME>}|load-image-status|versions {on <DEVICE-OR-
DOMAIN-NAME>}]
show device-upgrade status {on [<DOMAIN-NAME>/rf-domain-manager]/summary {on <DOMAIN-
NAME>}}
```

#### Parameters

```
show device-upgrade [history {on <DOMAIN-NAME>}|load-image-status|versions {on <DEVICE-OR-
DOMAIN-NAME>}]
```

|                                                  |                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| device-upgrade                                   | Displays firmware upgrade information based on the parameters passed                                                                                                                                                                                                                                                         |
| history {on<br><DOMAIN-<br>NAME>}                | Displays firmware upgrade history <ul style="list-style-type: none"> <li>on &lt;DOMAIN-NAME&gt; - Optional. Displays upgrade history for all devices within a specified RF Domain. Specify the RF Domain name.</li> </ul>                                                                                                    |
| load-image-<br>status                            | Displays firmware image loading status. The output displays the <DEVICE> image loading status in percentage.<br>For example,<br>#show device-upgrade load-image-status<br>Download of ap81xx firmware file is 47 percent complete                                                                                            |
| versions {on<br><DEVICE-OR-<br>DOMAIN-<br>NAME>} | Displays firmware image versions <ul style="list-style-type: none"> <li>on &lt;DEVICE-OR-DOMAIN-NAME&gt; - Optional. Displays firmware image versions loaded on specified device or RF Domain.</li> <li>&lt;DEVICE-OR-DOMAIN-NAME&gt; - Specify the AP, wireless controller, service platform, or RF Domain name.</li> </ul> |

```
show device-upgrade status {on [<DOMAIN-NAME>/rf-domain-manager]/summary {on <DOMAIN-NAME>}}
```

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| device-upgrade                           | Displays firmware upgrade information based on the parameters passed                                                                                                                                                                                                                                                                                                                                |
| status                                   | Displays in-progress device upgrade status                                                                                                                                                                                                                                                                                                                                                          |
| on [<DOMAIN-NAME> <br>rf-domain-manager] | Optional. Displays in progress upgrade status of all devices within a specified RF Domain, or all devices upgraded by the RF Domain manager. Use this option to view upgrade status of multiple devices. <ul style="list-style-type: none"> <li>&lt;DOMAIN-NAME&gt; - Specify the RF Domain name.</li> <li>rf-domain-manager - Select to view devices upgraded by the RF Domain manager.</li> </ul> |
| summary {on<br><DOMAIN-NAME>}            | Displays a summary of in-progress upgrade processes <ul style="list-style-type: none"> <li>on &lt;DOMAIN-NAME&gt; - Optional. Displays in-progress upgrade processes within a specified RF Domain</li> <li>&lt;DOMAIN-NAME&gt; - Specify the RF Domain name.</li> </ul>                                                                                                                             |

## Examples

```
nx9500-6C8809#device-upgrade load-image NX75xx ftp://anonymous:anonymous@192.168.13.10/
LatestBuilds/W592/NX75XX-LEAN.img
nx9500-6C8809#show device-upgrade load-image-status
Download of rfs6000 firmware file is complete
```

```
nx9500-6C8809#
nx9500-6C8809#show device-upgrade status
Number of devices currently being upgraded : 0
Number of devices waiting in queue to be upgraded : 1
Number of devices currently being rebooted : 0
Number of devices waiting in queue to be rebooted : 0
Number of devices failed upgrade : 0
```

```

 DEVICE STATE UPGRADE TIME REBOOT TIME PROGRESS RETRIES LAST UPDATE ERROR
UPGRADED BY

```

```
nx75xx-12E4c0 waiting immediate immediate 0 0 -
nx9500-6C8809

```

```
nx9500-6C8809#
```

## dot1x

Displays dot1x information on interfaces.

Dot1x (or 802.1x) is an IEEE standard for network authentication. Devices supporting dot1x allow the automatic provision and connection to the wireless network without launching a Web browser at login. When within range of a dot1x network, a device automatically connects and authenticates without needing to manually login.

However, dot1x-enabled devices can be configured either as:

- supplicants only – Devices seeking network access
- authenticators only – Devices authenticating the supplicants, or
- supplicants as well authenticators

---

### Note

Dot.1x supplicant configuration is supported on the following platforms:



- Access Points – AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP8163, AP8432, AP8533
- Wireless Controllers – RFS4000
- Service Platforms – NX5500, NX7500

---

### Note

Dot.1x authenticator configuration is supported on the following platforms:



- Access Points – AP6522, AP6562, AP7161, AP7502, AP8163
- Wireless Controllers – RFS4000
- Service Platforms – NX5500, NX7500

---

### Supported in the following platforms:

- Access Points – AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers – RFS 4000
- Service Platforms – NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show dot1x {all/interface/on}
show dot1x {all {on <DEVICE-NAME>}/on <DEVICE-NAME>}
show dot1x {interface [<INTERFACE-NAME>/ge <1-4>/port-channel <1-2>} {on <DEVICE-NAME>}
```

### Parameters

```
show dot1x {all {on <DEVICE-NAME>}/on <DEVICE-NAME>}
```

|                              |                                                                                                                                                                                                                                                                                                                       |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dot1x all {on <DEVICE-NAME>} | Optional. Displays dot1x information for all interfaces <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; - Optional. Displays dot1x information for all interfaces on a specified device</li> <li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |
| dot1x {on <DEVICE-NAME>}     | Optional. Displays dot1x information for interfaces on a specified device <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; - Specify the name of AP, wireless controller, or service platform.</li> </ul>                                                                                                   |

show dot1x {interface [<INTERFACE-NAME>/ge <1-4>/port-channel <1-2>]} {on <DEVICE-NAME>}

|                    |                                                                                                                                                                                                                                                                                                                    |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dot1x interface    | Optional. Displays dot1x information for a specified interface or interface type                                                                                                                                                                                                                                   |
| <INTERFACE-NAME>   | Displays dot1x information for the layer 2 (Ethernet port) interface specified by the <INTERFACE-NAME> parameter                                                                                                                                                                                                   |
| ge <1-4>           | Displays dot1x for a specified GigabitEthernet interface <ul style="list-style-type: none"> <li>&lt;1-4&gt; - Select the interface index from 1 - 4.</li> </ul>                                                                                                                                                    |
| port-channel <1-2> | Displays dot1x for a specified port channel interface <ul style="list-style-type: none"> <li>&lt;1-2&gt; - Select the interface index from 1 - 2.</li> </ul>                                                                                                                                                       |
| on <DEVICE-NAME>   | The following keywords are common to all of the above parameters: <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; - Optional. Displays dot1x interface information on a specified device</li> <li>&lt;DEVICE-NAME&gt; - Specify the name of AP, wireless controller, or service platform.</li> </ul> |

## Examples

```
ap8432-070235>show dot1x all
802.1X information

 SysAuthControl : disabled
 Guest-Vlan : disabled
 AAA-Policy : none
 Holdtime : 60

802.1X information for interface GE1

Supplicant MAC N/A
 Auth SM State : FORCE AUTHORIZED
 Bend SM State : REQUEST
 Port Status : AUTHORIZED
 Host Mode : SINGLE
 Auth Vlan : None
 Guest Vlan : None

802.1X information for interface GE2

Supplicant MAC N/A
 Auth SM State : FORCE AUTHORIZED
 Bend SM State : REQUEST
 Port Status : AUTHORIZED
 Host Mode : SINGLE
 Auth Vlan : None
 Guest Vlan : None

ap8432-070235>
```

## dpi

Displays DPI (Deep Packet Inspection) statistics for all configured and canned applications. DPI is an advanced packet analysis technique, which analyzes packet and packet content headers to determine the nature of network traffic. When DPI is enabled, packets of all flows are subjected to DPI to get accurate results. DPI identifies applications (such as, Netflix, Twitter, Facebook, etc.) and also extracts metadata (such as, host name, server name, TCP-RTT, etc.) for further use by the WiNG firewall.



### Note

The **show > dpi** command returns results only if executed on a device that supports DPI and has DPI logging enabled. DPI logging can be enabled either on the device or on the profile applied to the device. For more information, see [dpi](#) on page 986 (profile config mode).

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show dpi [app|app-category|application|application-policy|per-category]
show dpi app wireless-clients stats <MAC> {on <DEVICE-OR-DOMAIN-NAME>}
show dpi [app|app-category] stats [<APPLICATION/APP-CATEGORY-NAME>|all] {on <DEVICE-OR-DOMAIN-NAME>}
show dpi application-policy stats <APPLICATION-POLICY-NAME> {on <DEVICE-OR-DOMAIN-NAME>}
show dpi application brief
show dpi per-category stats <APP-CATEGORIES> [bytes-in|bytes-out|total-bytes] {on <DEVICE-OR-DOMAIN-NAME>}
```

### Parameters

```
show dpi app wireless-clients stats <MAC> {<DEVICE-OR-DOMAIN-NAME>}
```

|                                |                                                                                                                                                                                                                                                     |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dpi app wireless-clients <MAC> | Displays application-related statistics for all or a specified wireless clients <ul style="list-style-type: none"><li>• &lt;MAC&gt; - Displays statistics for a specified wireless client. Specify the client's MAC address.</li></ul>              |
| on <DEVICE-OR-DOMAIN-NAME>     | Optional. Displays statistical data on a specified device or RF Domain <ul style="list-style-type: none"><li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; - Specify the name of the access point, wireless controller, service platform, or RF Domain.</li></ul> |

```
show dpi [app|app-category] stats [<APPLICATION/APP-CATEGORY-NAME>|all]
{on <DEVICE-OR-DOMAIN-NAME>}
```

|                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>dpi [app  app-category] stats</pre>               | <p>Displays statistics for a application or application category</p> <ul style="list-style-type: none"> <li>• app – Displays statistics for a specified application or all applications</li> <li>• app-category – Displays statistics for a specified application category or all categories.</li> </ul> <p><b>Note:</b> The applications are the RF Domain member allowed applications whose data (bytes) are passing through the WiNG managed network. And, the application categories are existing WiNG or user defined application groups (video, streaming, mobile, audio, etc.) that assist administrators to permit or deny forwarding of application data.</p> |
| <pre>[&lt;APPLICATION/APP-CATEGORY-NAME&gt; all]</pre> | <p>This parameter is common to the 'app' and 'app-category' keywords.</p> <ul style="list-style-type: none"> <li>• &lt;APPLICATION/APP-CATEGORY-NAME&gt; – Displays statistics for a specified application or application category, depending on the option selected in the previous step. Specify the application name or application category name.</li> <li>• all – Displays statistics for all applications or application categories, depending on the option selected in the previous step</li> </ul>                                                                                                                                                            |
| <pre>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</pre>            | <p>Optional. Displays statistical data on a specified device or RF Domain</p> <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the access point, wireless controller, service platform, or RF Domain.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                           |

```
show dpi application-policy stats <APPLICATION-POLICY-NAME> {on <DEVICE-OR-DOMAIN-NAME>}
```

|                                             |                                                                                                                                                                                                                                                                                         |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>dpi application-policy stats</pre>     | <p>Displays statistics for an existing application policy</p>                                                                                                                                                                                                                           |
| <pre>&lt;APPLICATION-POLICY-NAME&gt;</pre>  | <p>Displays statistics for a specified application-policy. Specify the application-policy name.</p>                                                                                                                                                                                     |
| <pre>on &lt;DEVICE-OR-DOMAIN-NAME&gt;</pre> | <p>Optional. Displays application-policy related statistical data on a specified device or RF Domain</p> <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the access point, wireless controller, service platform, or RF Domain.</li> </ul> |

```
show dpi application brief
```

|                                  |                                                                                |
|----------------------------------|--------------------------------------------------------------------------------|
| <pre>dpi application brief</pre> | <p>Displays a brief summary of applications their status and configuration</p> |
|----------------------------------|--------------------------------------------------------------------------------|

```
show dpi per-category stats <APP-CATEGORIES> [bytes-in|bytes-out|total-bytes]
{on <DEVICE-OR-DOMAIN-NAME>}
```

|                                   |                                                                                                                                                                                   |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>dpi per-category stats</pre> | <p>Displays statistics for the top ten applications based on the application category and the Sort ID specified. The Sort ID options are: bytes-in, bytes-out or total-bytes.</p> |
| <pre>&lt;APP-CATEGORIES&gt;</pre> | <p>Specify the application category name. The system displays statistics for the top ten applications in this category.</p>                                                       |

[bytes-in|bytes-out| total-bytes]

Filters and displays statistical data for the top ten utilized applications in respect to the following:

- bytes-in - Displays total data bytes uploaded through the controller managed network. If this application data is not aligned with application utilization expectations, consider allowing or denying additional applications and categories or adjusting their precedence (priority).
- bytes-out - Displays total data bytes downloaded through the controller managed network. If this application data is not aligned with application utilization expectations, consider allowing or denying additional applications and categories or adjusting their precedence (priority).
- total-bytes - Displays total data bytes (uploaded and downloaded) through the controller managed network. These are only the administrator allowed applications approved for proliferation within the managed network.

on <DEVICE-OR-DOMAIN-NAME>

Optional. Displays statistical data on a specified device or RF Domain

- <DEVICE-OR-DOMAIN-NAME> - Specify the name of the access point, wireless controller, service platform, or RF Domain.

## Examples

```
nx9500-6C8809>show dpi application brief
 1-clickshare-com
 This application recognizes DirectDownloadLink 1-clickshare
 traffic
 Application Category : filetransfer
 Predefined Application : Yes
 1-upload-com
 This application recognizes DirectDownloadLink 1-upload-com
 traffic
 Application Category : filetransfer
 Predefined Application : Yes
 1-upload-to
 This application recognizes DirectDownloadLink 1-upload-to
 traffic
 Application Category : filetransfer
 Predefined Application : Yes
 10upload-com
 This application recognizes DirectDownloadLink 10upload-com
 traffic
 Application Category : filetransfer
 Predefined Application : Yes
 123upload-pl
 This application recognizes DirectDownloadLink 123upload-pl
 traffic
--More--
nx9500-6C8809>
```

## Related Commands

|  |
|--|
|  |
|  |

*eguest*

Displays EGuest server status and EGuest registration statistics



## Supported in the following platforms:

- Service Platforms — NX 95XX, VX 9000

## Syntax

```
eguest [registration statistics|status]
```

## Parameters

```
eguest [registration statistics|status]
```

|                         |                                               |
|-------------------------|-----------------------------------------------|
| registration statistics | Displays the EGuest registration statistics   |
| status                  | Displays the current status of EGuest servers |

## Examples

```
vx-eguest-primary#show eguest status
```

```

pid process

2521 gmd
2529 regserver
2539 acct_server
2569 guest_manager
2636 acct_server
2642 acct_server
2643 acct_server
2649 acct_server
2655 acct_server
2708 acct_server-helper
2770 guest_manager
2776 guest_manager
2777 guest_manager
2783 guest_manager
3628 gmd
3630 gmd
3631 gmd
3632 gmd
3633 gmd
3634 gmd
5729 radiusd

```

```
Database server is local
```

```
Database server is reachable
```

```
vx-eguest-primary#
```

```
vx-eguest-primary#show eguest registration statistics
```

```
msg_received - number of registration messages received
```

```
user_try_to_add - number of database add attempts
```

```
user_added - number of messages succesfully added to db
```

```
user_failed - number of messages failed adding to db
```

```

msg_received user_try_to_add user_added user_failed

```

```
189 11 11 0
```

```
vx-eguest-primary#
```

## environmental-sensor

Displays environmental sensor's recorded data. The environmental sensor has to be enabled and configured in order to collect data related to humidity, light, motion, and temperature.



### Note

The environmental sensor is supported only on an AP 8132. When executed on any controller (other than an AP 8132), the **show > environmental-sensor > <parameters>** command displays environmental-sensor details for adopted AP 8132s (if any).

### Supported in the following platforms:

- AP 8132

### Syntax

```
show environmental-sensor [history|humidity|light|motion|summary|temperature|version]
```

```
show environmental-sensor history {<1-HOUR>|<20-MINUTE>|<24-HOUR>}
```

```
show environmental-sensor [humidity|light|motion|summary|temperature|version]
```

### Parameters

```
show environmental-sensor history {<1-HOUR>|<20-MINUTE>|<24-HOUR>}
```

|                              |                                                                                                                                                                                                          |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| environmental-sensor history | Displays environmental sensor history once in every hour, 20 minutes, or 24 hours. History includes the humidity, light, motion, and temperature data recorded by the sensor at specified time interval. |
| 1 hour                       | Optional. Displays environmental sensor history once in every 1 (one) hour.                                                                                                                              |
| 20-minute                    | Optional. Displays environmental sensor history once in every 20 minutes.                                                                                                                                |
| 24-hour                      | Optional. Displays environmental sensor history once in every 24 hours.                                                                                                                                  |

```
show environmental-sensor [humidity|light|motion|summary|temperature|version]
```

|                      |                                                                                                                                                                                                                                     |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| environmental-sensor | Displays environmental sensor's recorded data, based on the parameters passed. The system displays the specified recorded data. The environmental sensor records data at the following intervals: 20 minutes, 1 hour, and 24 hours. |
| humidity             | Displays the minimum, average, and maximum humidity recorded.                                                                                                                                                                       |
| light                | Displays the minimum, average, and maximum light recorded.                                                                                                                                                                          |
| motion               | Displays the minimum, average, and maximum motion recorded.                                                                                                                                                                         |
| temperature          | Displays the minimum, average, and maximum temperature recorded.                                                                                                                                                                    |
| version              | Displays the hardware and firmware versions.                                                                                                                                                                                        |
| summary              | Displays a summary of the data recorded at following intervals:                                                                                                                                                                     |

### Examples

```
ap8132-711728#show environmental-sensor summary
Maat Device uptime: 0 days 15:25:11
ERROR: Maat device is offline!
threshold polling-interval: 5
historical data polled 0 times per 2-minutes interval since Maat online
motion-sensor: Enabled(Demo)
 current value: 0 detected
```

-----  
motion detected  
-----

20-minute 0  
1-hour 0  
6-hour 0  
24-hour 0

temperature-sensor: Enabled(Demo)  
current value: -40.00 deg. C  
-----

min/average/max  
-----

20-minute 0/0/0  
1-hour 0/0/0  
6-hour 0/0/0  
24-hour 0/0/0

light-sensor: Enabled  
threshold-high:+400.00 threshold-low:+200.00 holdtime:11  
action radio-shutdown: radio-1 and radio-2  
light-on:1  
light-on/off event sent:0/0  
current value: 0.00 lux  
-----

min/average/max  
-----

20-minute 0/0/0  
1-hour 0/0/0  
6-hour 0/0/0  
24-hour 0/0/0

humidity-sensor: Enabled(Demo)  
current value: 0.00 %  
-----

min/average/max  
-----

20-minute 0/0/0  
1-hour 0/0/0  
6-hour 0/0/0  
24-hour 0/0/0

ap8132-711728#  
ap8132-711634#show env-sensor history  
Current Time: 2015-06-20 14:08:01 UTC  
-----

| Sample-Interval             | Motion | Temperature<br>(deg. C) | Light<br>(lux) | Humidity<br>(%) |
|-----------------------------|--------|-------------------------|----------------|-----------------|
| ----- min/average/max ----- |        |                         |                |                 |
| 20-minute                   | 1      | 64/65/66                | 77/80          | 58/60/61        |
| 1-hour                      | 24     | 63/67/70                | 75/81          | 57/59/61        |
| 6-hour                      | 128    | 60/62/69                | 71/79          | 52/56/71        |
| 24-hour                     | 188    | 54/58/70                | 15/45          | 49/57/73        |

ap8132-711634#  
ap8132-711634#show env-sensor history 20-min  
-----

| timestamp               | Motion | Temperature | Light | Humidity |
|-------------------------|--------|-------------|-------|----------|
| -----                   |        |             |       |          |
| 2015-11-20 13:51:35 UTC | 0      | 66          | 79    | 59       |
| 2015-11-20 13:53:35 UTC | 0      | 66          | 79    | 59       |
| 2015-11-20 13:55:35 UTC | 0      | 65          | 79    | 58       |
| 2015-11-20 13:57:35 UTC | 1      | 66          | 80    | 59       |
| 2015-11-20 13:59:35 UTC | 0      | 66          | 79    | 59       |
| 2015-11-20 14:02:35 UTC | 0      | 65          | 79    | 60       |
| 2015-11-20 14:03:35 UTC | 0      | 64          | 79    | 60       |
| 2015-11-20 14:05:35 UTC | 2      | 66          | 80    | 60       |
| 2015-11-20 14:07:35 UTC | 0      | 66          | 80    | 61       |

```

2015-11-20 14:09:35 UTC 0 66 80 61
ap8132-711634#
ap8132-711634#show env-sensor history 1-hr

```

```

timestamp Motion Temperature Light Humidity

2015-11-20 13:51:35 UTC 0 66 79 59
2015-11-20 13:53:35 UTC 0 66 79 59
2015-11-20 13:55:35 UTC 0 65 79 58
2015-11-20 13:57:35 UTC 1 66 80 59
2015-11-20 13:59:35 UTC 0 66 79 59
2015-11-20 14:01:35 UTC 0 65 79 60
2015-11-20 14:03:35 UTC 0 64 79 60
2015-11-20 14:05:35 UTC 2 66 80 60
2015-11-20 14:07:35 UTC 0 66 80 61
2015-11-20 14:09:35 UTC 0 66 80 61
2015-11-20 14:42:35 UTC 0 65 81 60
2015-11-20 14:43:35 UTC 0 64 80 59
2015-11-20 14:45:35 UTC 3 66 80 60

```

```

ap8132-711634#
<DEVICE-NAME>#show env-sensor history 24-hr

```

```

timestamp Motion Temperature Light Humidity

2015-11-20 10:10:20 UTC 27 66 80 60
2015-11-20 10:30:20 UTC 17 66 80 60
2015-11-20 10:50:20 UTC 17 66 81 60
2015-11-20 11:10:20 UTC 25 66 81 60
2015-11-20 11:30:20 UTC 24 66 81 60
2015-11-20 11:50:20 UTC 26 66 81 60
2015-11-21 08:10:20 UTC 9 65 80 59
2015-11-21 08:30:20 UTC 7 65 80 59
2015-11-21 08:50:20 UTC 12 65 80 60
2015-11-21 09:10:20 UTC 10 65 80 60
2015-11-21 09:30:20 UTC 15 65 80 60
2015-11-21 09:50:20 UTC 19 66 80 60
<DEVICE-NAME>#

```

### event-history

Displays event history report

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
show event-history {on <DEVICE-OR-DOMAIN-NAME>}
```

#### Parameters

```
show event-history {on <DEVICE-OR-DOMAIN-NAME>}
```

|                            |                                                                                                                                                                                                                                       |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| event-history              | Displays event history report                                                                                                                                                                                                         |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Displays event history report on a device or RF Domain <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; - Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> |

## Examples

```
nx9500-6C8809#show event-history
Generated on '2016-09-21 05:19:55 UTC' by 'admin'

2017-06-06 10:40:19 nx9500-6C8809 SYSTEM LOGIN
Successfully logged in user 'admin' with privilege 'superuser' from 'ssh'
2017-06-06 10:38:36 nx9500-6C8809 SYSTEM LOGOUT
Logged out user 'admin' with privilege 'superuser' from '192.168.100.214'
2017-06-06 10:27:34 nx9500-6C8809 SYSTEM LOGIN
Successfully logged in user 'admin' with privilege 'superuser' from 'ssh'
2017-06-06 10:27:34 nx9500-6C8809 SYSTEM LOGOUT
Logged out user 'admin' with privilege 'superuser' from '192.168.100.214'
2016-09-20 23:52:49 nx9500-6C8809 SYSTEM LOGIN
Successfully logged in user 'admin' with privilege 'superuser' from 'ssh'
2016-09-20 05:39:01 nx9500-6C8809 SYSTEM LOGOUT
Logged out user 'admin' with privilege 'superuser' from '192.168.100.165'
2016-09-20 05:08:54 nx9500-6C8809 SYSTEM LOGIN
Successfully logged in user 'admin' with privilege 'superuser' from 'ssh'
--More--
nx9500-6C8809#
```

### *event-system-policy*

Displays detailed event system configuration

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
show event-system-policy [config|detail] <EVENT-SYSTEM-POLICY-NAME>
```

#### Parameters

```
show event-system-policy [config|detail] <EVENT-SYSTEM-POLICY-NAME>
```

|                             |                                                        |
|-----------------------------|--------------------------------------------------------|
| event-system-policy         | Displays event system policy configuration             |
| config                      | Displays configuration for a specified policy          |
| detail                      | Displays detailed configuration for a specified policy |
| <EVENT-SYSTEM- POLICY-NAME> | Specify the event system policy name.                  |

#### Examples

```
nx9500-6C8809(config)#show event-system-policy config testpolicy
```

```

MODULE EVENT SYSLOG SNMP FORWARD EMAIL

aaa radius-discon-msg on on on default

nx9500-6C8809(config)#
```

### *ex3500*

Displays EX3500-related statistical data

## Supported in the following platforms:

- Service Platforms — NX 7510, NX 95XX

## Syntax

```
show ex3500 [dir|interfaces|system|upgrade|version|whichboot]
show ex3500 dir {boot-rom/config/on/opcode} {<FILE-NAME>} {on <EX3500-DEVICE-NAME>}
show ex3500 interfaces counters [ether-like stats|ethernet <1-1> <1-52>|
ext-if-table stats|if-table stats|portUtil stats|rmon stats] {on <EX3500-DEVICE-NAME>}
show ex3500 [system|upgrade|version|whichboot] {on <EX3500-DEVICE-NAME>}
```

## Parameters

```
show ex3500 dir {boot-rom/config/on/opcode} {<FILE-NAME>} {on <EX3500-DEVICE-NAME>}
```

|                         |                                                                                                                                                                                                                                     |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ex3500 dir              | Displays EX3500 directory information based on the option selected. The options are: boot-rom, config, opcode<br><br><b>Note:</b> If none of the specified options is selected, all EX3500 system-related information is displayed. |
| boot-rom                | Optional. Displays only the Boot-ROM information                                                                                                                                                                                    |
| config                  | Optional. Displays only the configuration file                                                                                                                                                                                      |
| opcode                  | Optional. Displays only the run-time operation code                                                                                                                                                                                 |
| <FILE-NAME>             | Displays the contents of a specified file identified by the <FILE-NAME> keyword. This is the name of configuration file or code image.                                                                                              |
| on <EX3500-DEVICE-NAME> | Optional. Executes the command on a specified EX3500 device <ul style="list-style-type: none"><li>• &lt;DEVICE-NAME&gt; - Specify the device's name.</li></ul>                                                                      |

```
show ex3500 interfaces counters [ether-like stats|ethernet <1-1> <1-52>|
ext-if-table stats|if-table stats|portUtil stats|rmon stats] {on <EX3500-DEVICE-NAME>}
```

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ex3500 interfaces counters | Displays EX3500 interface counter information based on the option selected. The options are: ether-like, ethernet, ext-if-table, if-table, portUtil, rmon                                                                                                                                                                                                                                                                                                                                                                                               |
| ether-like stats           | Displays MIB (Managed Information Base) object statistics for Ethernet-like interfaces                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| ethernet <1-1> <1-52>      | Displays the Ethernet port statistics based on the unit identifier and port number selected <ul style="list-style-type: none"><li>• &lt;1-1&gt; - Specify the EX3500 unit's identifier from 1 - 1.</li><li>• &lt;1-52&gt; - Specify the port number from 1 - 52. This range varies for the EX3524 (1-28) and EX3548 (1-52) devices.</li></ul><br><b>Note:</b> This option displays the following for the selected Ethernet interface: extended interface table stats, interface table stats, port utilization information, and remote monitoring stats. |
| ext-if-table stats         | Displays only the extended interface table statistics                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| if-table stats             | Displays only the interface table statistics                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| portUtil stats             | Displays only the port utilization information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

|                         |                                                                                                                                                                |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| rmon stats              | Displays only RMon (remote monitoring) statistics                                                                                                              |
| on <EX3500-DEVICE-NAME> | Optional. Executes the command on a specified EX3500 device <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; - Specify the device's name.</li> </ul> |

show ex3500 [system|upgrade|version|whichboot] {on <EX3500-DEVICE-NAME>}

|                         |                                                                                                                                                                                                                                                |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ex3500                  | Displays the following information for a specified EX3500 device or all EX3500 devices in the managed network                                                                                                                                  |
| system                  | Displays EX3500 system information, such as device description, OID string, up time, name, location, contact, MAC address, etc. Some of these information (example, system name) are configurable items, and if not configured are left blank. |
| upgrade                 | Displays the opcode upgrade configuration settings                                                                                                                                                                                             |
| version                 | Displays hardware and software version information for a EX3500 system                                                                                                                                                                         |
| whichboot               | Displays boot information                                                                                                                                                                                                                      |
| on <EX3500-DEVICE-NAME> | Optional. Executes the command on a specified EX3500 device <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; - Specify the device's name.</li> </ul>                                                                                 |

## Examples

```

nx9500-6C8809#show ex3500 interfaces counters ethernet 1 17
Ethernet 1/ 17
===== IF table Stats =====
2166458 Octets Input
14734059 Octets Output
14707 Unicast Input
19806 Unicast Output
0 Discard Input
0 Discard Output
0 Error Input
0 Error Output
0 Unknown Protocols Input
0 QLen Output
===== Extended Iftable Stats =====
23 Multi-cast Input
5525 Multi-cast Output
170 Broadcast Input
11 Broadcast Output
===== Ether-like Stats =====
0 Alignment Errors
0 FCS Errors
0 Single Collision Frames
0 Multiple Collision Frames
0 SQE Test Errors
0 Deferred Transmissions
0 Late Collisions
0 Excessive Collisions
0 Internal Mac Transmit Errors
0 Internal Mac Receive Errors
0 Frames Too Long
0 Carrier Sense Errors
0 Symbol Errors
0 Pause Frames Input
0 Pause Frames Output
===== RMON Stats =====
0 Drop Events
16900558 Octets

```

```

40243 Packets
170 Broadcast PKTS
23 Multi-cast PKTS
0 Undersize PKTS
0 Oversize PKTS
0 Fragments
0 Jabbers
0 CRC Align Errors
0 Collisions
21065 Packet Size <= 64 Octets
3805 Packet Size 65 to 127 Octets
2448 Packet Size 128 to 255 Octets
797 Packet Size 256 to 511 Octets
2941 Packet Size 512 to 1023 Octets
9187 Packet Size 1024 to 1518 Octets
==== Port Utilization (recent 300 seconds) ====
0 Octets Input in kbits per second
0 Packets Input per second
0.00 % Input Utilization
0 Octets Output in kbits per second
0 Packets Output per second
0.00 % Output Utilization
nx9500-6C8809#

```

### *extdev*

Displays external device (T5 or EX3500) configuration error history

#### **Supported in the following platforms:**

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX

#### **Syntax**

```
show extdev error history {on <T5/EX3500-DEVICE-NAME>}
```

#### **Parameters**

```
show extdev error history {on <T5/EX3500-DEVICE-NAME>}
```

|                            |                                                                                                                                                                                                                                                                                            |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| extdev error history       | Displays external device error history. This command is applicable only to the external devices T5, and EX3500 series switches. Use this command to view configuration error history for all or a specified external device adopted and managed by a WiNG NX 95XX series service platform. |
| on <T5/EX3500-DEVICE-NAME> | Optional. Displays configuration error history on a specified T5 or EX3500 device <ul style="list-style-type: none"> <li>• &lt;T5/EX3500-DEVICE-NAME&gt; - Specify the name of the device.</li> </ul>                                                                                      |

#### **Examples**

```

nx9500-6C8809#show extdev error history on t5-ED5EAC
%% No History for this device
nx9500-6C8809#

```

### *fabric-attach*

Displays the current status of FA (Fabric Attach) VLAN to I-SID (Individual Service Identifier) assignments for all ports.



### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show fabric-attach assignments {on <DEVICE-NAME>}
```

### Parameters

```
show fabric-attach assignments {on <DEVICE-NAME>}
```

|                  |                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| fabric-attach    | Displays the status of VLAN to I-SID mappings, if configured, on the Ethernet ports of an FA Client. The status displays as: <ul style="list-style-type: none"><li>• active – If the VLAN to I-SID mapping is accepted by the FA Server and applied to the VLAN traffic from the client.</li><li>• pending – If the VLAN to I-SID mapping acceptance is not achieved (i.e, pending acceptance)</li></ul> |
| on <DEVICE-NAME> | Optional. Displays VLAN to I-SID mappings on a specified FA client. If executing this command on a controller, you may, optionally, specify the device for which the FA VLAN to I-SID assignments is to be displayed. <ul style="list-style-type: none"><li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li></ul>                                      |

### Example

The Following example shows the fabric-attach VLAN to ISID assignment configured on the ap7532-000100 access point:

```
nx9600-7F3B2C#
ap7532 B8-50-01-00-01-00
 use profile default-ap7532
 use rf-domain default
 hostname ap7532-000100
 interface gel
 switchport mode trunk
 switchport trunk fabric-attach vlan 110 isid 10180110
 switchport trunk native vlan 110
 switchport trunk native tagged
 switchport trunk allowed vlan 110
 interface vlan110
 ip address dhcp
 ip dhcp client request options all
nx9600-7F3B2C#
```

The following example shows the fabric-attach assignment status for the ap7532-000100 access point:

```
nx9600-7F3B2C#show fabric-attach assignments on ap7532-000100

Assignment status for port : gel
VLAN ISID STATUS
---- -
110 10180110 Accepted

nx9600-7F3B2C#
```

file

Displays file system information



#### Note

This command is not available in the USER EXEC mode.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
show file [information <FILE>|systems]
```

#### Parameters

```
show file [information <FILE>|systems]
```

|                    |                                                                                                                   |
|--------------------|-------------------------------------------------------------------------------------------------------------------|
| information <FILE> | Displays file information <ul style="list-style-type: none"><li>• &lt;FILE&gt; - Specify the file name.</li></ul> |
| systems            | Lists all file systems present in the system                                                                      |

#### Examples

```
ap8432-070235#show file systems
```

```
File Systems:
```

| Size(Mb) | Free(Mb) | Use% | Type  | Prefix |
|----------|----------|------|-------|--------|
| 64       | 62       | 3    | flash | nvrn:  |
| 84       | 81       | 2    | flash | flash: |
| 137      | 82       | 40   | -     | vmsdb: |

```
ap8432-070235#
```

```
nx9500-6C8809#show file information startup-config
```

```
nvrn:startup-config:
```

```
type is configuration file
```

```
nx9500-6C8809#
```

file-sync

Displays file synchronization settings and status on a controller

The file-sync command syncs wireless-bridge certificate and trustpoint between the staging-controller and its adopted access points. The **show > file-sync** command displays information related to this process.

#### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 7510, NX 95XX, NX 96XX

#### Syntax

```
show file-sync [configuration|history|load-file-status|status] {on <DEVICE-OR-DOMAIN-NAME>}
```

## Parameters

```
show file-sync [configuration|history|load-file-status|status] {on <DEVICE-OR-DOMAIN-NAME>}
```

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| file-sync                   | Displays the following file-synchronization (trustpoint and wireless-bridge certificate) related information: configuration, history, load-file-status, and status                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| configuration               | <p>Displays the following file-synchronization configuration details:</p> <ul style="list-style-type: none"><li>• automatic file-syncing enabled or disabled. The default setting is disabled.</li></ul> <p>The X.509 certificate needs synchronization only if the access point's radio2 is configured to use EAP-TLS authentication. In which case PKCS#12 certificate needs to be pushed on AP adoption. To enable automatic file syncing, in the controller's device/profile configuration mode, execute the <b>file-sync &gt; auto</b> command. For more information, see <a href="#">file-sync</a> on page 999 (profile config mode).</p> <ul style="list-style-type: none"><li>• Number of access points to which the certificate can be simultaneously uploaded. The default is 10.</li></ul> <p>To modify the number of simultaneous uploads, in the controller's device/profile configuration mode, execute the <b>file-sync &gt; count &lt;1-20&gt;</b> command. For more information, see <a href="#">file-sync</a> on page 999 (profile config mode).<li>• Scheduled certificate upload, if any, details, such time and date of upload.</li><p>To schedule certificate upload, use the <b>file-sync &gt; wireless-certificate</b> command. For more information, see <a href="#">file-sync</a> on page 999 (profile config mode).</p></p> |
| history                     | Displays file synchronization history. Use this option to view statistical data relating to wireless-bridge certificate synchronization between staging controller and its access points. When executed, a list of all certificate transfers made to the APs is displayed, with the latest transfer listed at the top.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| load-file-status            | Displays the status of the file upload to the controller. Use this command to view the status of a in-progress certificate upload. For more information on initiating a PKCS#12 certificate upload, see <a href="#">file-sync</a> on page 999 (profile config mode).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| status                      | Displays status of the file synchronization between the controller and its adopted access point.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| on <DEVICE-OR-DOMAIN- NAME> | <p>Optional. Displays file synchronization settings and status on a specified device or RF Domain</p> <ul style="list-style-type: none"><li>• &lt;DEVICE-OR-DOMAIN- NAME&gt; – Specify the name of the controller, service platform, or RF Domain.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Examples

```
nx9500-6C8809#show file-sync configuration
File Sync Configuration Information
 Auto : Disabled
 Simultaneous Upload Count : 128
```

```

Wireless Bridge Cert Load Time : Thu May 29 23:23:35 2015
nx9500-6C8809#
nx9500-6C8809#show file-sync load-file-status
Download of wireless_bridge certificate is complete
nx9500-6C8809#
nx9500-6C8809#show file-sync history

 AP RESULT TIME RETRIES SYNCED-BY LAST-SYNC-ERROR

AP6522-491220 done 2015-05-27 01:37:32 B4-C7-99-6C-88-09 -
ME733ANACBMOT21 done 2015-05-27 02:02:51 0 B4-C7-99-6C-88-09 -
nx9500-6C8809#

```

## firewall

Displays wireless firewall information, such as DHCP (Dynamic Host Configuration Protocol) snoop table entries, denial of service statistics, active session summaries, etc.



### Note

This command is not available in the USER EXEC mode.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```

show firewall [dhcp|flows|neighbors]
show firewall dhcp snoop-table {on <DEVICE-NAME>}
show firewall flows {filter|management|on/stats/wireless-client}
show firewall flows {filter} {(dir|dst port <1-65535>|ether|flow-type|icmp|
icmpv6|igmp|ip|ipv6|max-idle|min-bytes|min-idle|min-pkts|not|port|src|tcp|udp)}
show firewall flows {management {on <DEVICE-NAME>}|stats {on <DEVICE-NAME>}|
wireless-client <MAC>|on <DEVICE-NAME>}
show firewall neighbors snoop-table {on <DEVICE-NAME>}

```

### Parameters

```
show firewall dhcp snoop-table {on <DEVICE-NAME>}
```

|                                              |                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| firewall dhcp snoop-table {on <DEVICE-NAME>} | <p>Displays DHCP snoop table entries</p> <ul style="list-style-type: none"> <li>• snoop-table - Displays DHCP snoop table entries</li> </ul> <p>DHCP snooping acts as a firewall between non-trusted hosts and the DHCP server. Snoop table entries contain MAC address, IP address, lease time, binding type, and interface information of non-trusted interfaces.</p> |
| on <DEVICE-NAME>                             | <p>The following keyword is common to the 'DHCP snoop table' and 'DoS stats' parameters:</p> <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; - Optional. Displays snoop table entries, or DoS stats on a specified device</li> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul>             |

```

show firewall flows {filter} {(dir|dst|ether|flow-type|icmp|icmpv6|igmp|ip|
ipv6|max-idle|min-bytes|min-idle|min-pkts|not|port|src|tcp|udp)}

```

|                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| firewall flows                                                       | Notifies a session has been established                                                                                                                                                                                                                                                                                                                                                                                             |
| filter                                                               | Optional. Defines additional firewall flow filter parameters                                                                                                                                                                                                                                                                                                                                                                        |
| dir [wired-wired  wired-wireless  wireless-wired  wireless-wireless] | Optional. Matches the packet flow direction <ul style="list-style-type: none"> <li>wired-wired – Wired to wired flows</li> <li>wired-wireless – Wired to wireless flows</li> <li>wireless-wired – Wireless to wired flows</li> <li>wireless-wireless – Wireless to wireless flows</li> </ul>                                                                                                                                        |
| dst port <1-65535>                                                   | Optional. Matches the destination port with the specified port <ul style="list-style-type: none"> <li>port &lt;1-65535&gt; – Specifies the destination port number from 1 - 65535</li> </ul>                                                                                                                                                                                                                                        |
| ether [dst <MAC>  host <MAC>  src <MAC>  vlan <1-4094>]              | Optional. Displays Ethernet filter options <ul style="list-style-type: none"> <li>dst &lt;MAC&gt; – Matches only the destination MAC address</li> <li>host &lt;MAC&gt; – Matches flows containing the specified MAC address</li> <li>src &lt;MAC&gt; – Matches only the source MAC address</li> <li>vlan &lt;1-4094&gt; – Matches the VLAN number of the traffic with the specified value. Specify a value from 1- 4094.</li> </ul> |
| flow-type [bridged natted routed  wired wireless]                    | Optional. Matches the traffic flow type <ul style="list-style-type: none"> <li>bridged – Bridged flows</li> <li>natted – Natted flows</li> <li>routed – Routed flows</li> <li>wired – Flows belonging to wired hosts</li> <li>wireless – Flows containing a mobile unit</li> </ul>                                                                                                                                                  |
| icmp {code type}                                                     | Optional. Matches flows with the specified ICMP (Internet Control Message Protocol) version 4 code and type <ul style="list-style-type: none"> <li>code – Matches flows with the specified ICMPv4 code</li> <li>type – Matches flows with the specified ICMPv4 type</li> </ul>                                                                                                                                                      |
| icmpv6 {code type}                                                   | Optional. Matches flows with the specified ICMP version 6 code and type <ul style="list-style-type: none"> <li>code – Optional. Matches flows with the specified ICMPv6 code</li> <li>type – Optional. Matches flows with the specified ICMPv6 type</li> </ul>                                                                                                                                                                      |
| igmp                                                                 | Optional. Matches IGMP (Internet Group Management Protocol) flows                                                                                                                                                                                                                                                                                                                                                                   |
| ip [dst <IP>  host <IP>  proto <0-254>  src <IP>]                    | Optional. Filters firewall flows based on the IPv4 parameters passed <ul style="list-style-type: none"> <li>dst &lt;IP&gt; – Matches destination IP address</li> <li>host &lt;IP&gt; – Matches flows containing IPv4 address</li> <li>proto &lt;0-254&gt; – Matches the IPv4 protocol number with the specified number</li> <li>src &lt;IPv4&gt; – Matches source IP address</li> </ul>                                             |
| ipv6 [dst <IPv6>  host <IPv6>  proto <0-254>  src <IPv6>]            | Optional. Filters firewall flows based on the IPv6 parameters passed <ul style="list-style-type: none"> <li>dst &lt;IPv6&gt; – Matches destination IPv6 address</li> <li>host &lt;IPv6&gt; – Matches flows containing IPv6 address</li> <li>proto &lt;0-254&gt; – Matches the IPv6 protocol number with the specified number</li> <li>src &lt;IPv6&gt; – Matches source IPv6 address</li> </ul>                                     |

|                          |                                                                                                                                    |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| max-idle <1-4294967295>  | Optional. Filters firewall flows idle for at least the specified duration. Specify a max-idle value from 1 - 4294967295 bytes.     |
| min-bytes <1-4294967295> | Optional. Filters firewall flows with at least the specified number of bytes. Specify a min-bytes value from 1 - 4294967295 bytes. |
| min-idle <1-4294967295>  | Optional. Filters firewall flows idle for at least the specified duration. Specify a min-idle value from 1 - 4294967295 bytes.     |
| min-pkts <1-4294967295>  | Optional. Filters firewall flows with at least the given number of packets. Specify a min-bytes value from 1 - 4294967295 bytes.   |
| not                      | Optional. Negates the filter expression selected                                                                                   |
| port <1-65535>           | Optional. Matches either the source or destination port. Specify a port from 1 - 65535.                                            |
| src <1-65535>            | Optional. Matches only the source port with the specified port. Specify a port from 1 - 65535.                                     |
| tcp                      | Optional. Matches TCP flows                                                                                                        |
| udp                      | Optional. Matches UDP flows                                                                                                        |

```
show firewall flows {management {on <DEVICE-NAME>}}/stats {on <DEVICE-NAME>}/
wireless-client <MAC>/on <DEVICE-NAME>}
```

|                               |                                                                                                                                                                                                                                                                                              |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| firewall flows                | Notifies a session has been established                                                                                                                                                                                                                                                      |
| management {on <DEVICE-NAME>} | Optional. Displays management traffic firewall flows <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; – Optional. Displays firewall flows on a specified device</li> <li>&lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul> |
| stats {on <DEVICE-NAME>}      | Optional. Displays active session summary <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; – Optional. Displays active session summary on a specified device</li> <li>&lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul>    |
| wireless-client <MAC>         | Optional. Displays wireless clients firewall flows <ul style="list-style-type: none"> <li>&lt;MAC&gt; – Specify the MAC address of the wireless client.</li> </ul>                                                                                                                           |
| on <DEVICE-NAME>              | Optional. Displays all firewall flows on a specified device <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul>                                                                                    |

```
show firewall neighbors snoop-table {on <DEVICE-NAME>}
```

|                                |                                                                                                                                                                                                                           |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| firewall neighbors snoop-table | Displays IPv6 neighbors snoop table entries                                                                                                                                                                               |
| on <DEVICE-NAME>               | Optional. Displays IPv6 neighbors snoop table entries on a specified device <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

### Examples

```
nx9500-6C8809(config)#show fi
file-sync firewall file
```

```

nx9500-6C8809(config)#show firewall dhcp snoop-table
Snoop Binding <192.168.13.24, 00-15-70-81-74-2D, Vlan 1>
Type switch-SVI, Touched 427779 seconds ago

nx9500-6C8809(config)#
nx9500-6C8809(config)#show firewall dos stats

```

| ATTACK TYPE              | COUNT | LAST OCCURENCE      |
|--------------------------|-------|---------------------|
| udp-short-hdr            | 0     | Never               |
| multicast-icmpv6         | 0     | Never               |
| icmp-router-solicit      | 0     | Never               |
| tcp-xmas-scan            | 0     | Never               |
| ascend                   | 0     | Never               |
| twinge                   | 0     | Never               |
| tcp-post-syn             | 0     | Never               |
| land                     | 0     | Never               |
| broadcast-multicast-icmp | 0     | Never               |
| ftp-bounce               | 0     | Never               |
| spoof                    | 0     | Never               |
| source-route             | 0     | Never               |
| tcp-null-scan            | 0     | Never               |
| tcp-fin-scan             | 0     | Never               |
| ipv6-hop-limit-zero      | 0     | Never               |
| tcp-bad-sequence         | 97    | 0 days 02:24:32 ago |
| fraggle                  | 0     | Never               |
| router-adv               | 0     | Never               |
| snork                    | 0     | Never               |
| raguard                  | 0     | Never               |

```

--More--
nx9500-6C8809(config)#
nx9500-6C8809(config)#show firewall flows management
===== Flow# 1 Summary =====
Forward:
IPv4 Vlan 1, TCP 192.168.13.10 port 1646 > 192.168.13.24 port 22
 00-02-B3-28-D1-55 > 00-15-70-81-74-2D, ingress port up1
 Egress port: <local>, Egress interface: vlan1, Next hop: <local> (00-15-70-81-74-2D)
 1170 packets, 99960 bytes, last packet 0 seconds ago
Reverse:
IPv4 Vlan 1, TCP 192.168.13.24 port 22 > 192.168.13.10 port 1646
 00-15-70-81-74-2D > 00-02-B3-28-D1-55, ingress port local
 Egress port: up1, Egress interface: vlan1, Next hop: 192.168.13.10 (00-02-B3-28-D1-55)
 873 packets, 98797 bytes, last packet 0 seconds ago
TCP state: Established
Flow times out in 1 hour 30 minutes

nx9500-6C8809(config)#
nx9500-6C8809(config)#show firewall flows stats
Active Flows 2
TCP/IPv4 flows 2
UDP/IPv4 flows 0
DHCP/IPv4 flows 0
ICMP/IPv4 flows 0
IPsec/IPv4 flows 0
TCP/IPv6 flows 0
UDP/IPv6 flows 0
DHCP/IPv6 flows 0
ICMP/IPv6 flows 0
IPsec/IPv6 flows 0
L3/Unknown flows 0
nx9500-6C8809(config)#

```

## global

Displays global information for network devices based on the parameters passed

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show global [device-list|domain]
show global device-list {filter {offline|online|rf-domain}}
show global device-list {filter {offline|online}}
show global device-list {filter rf-domain [<DOMAIN-NAME>/not <DOMAIN-NAME>]}
show global domain managers
```

### Parameters

```
show global device-list {filter {offline|online}}
```

|                        |                                                                                                                                                                                                                                                    |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| global device -list    | Displays global information for all network devices. Use the following keywords to specify additional filters: <b>offline</b> , <b>online</b> , and <b>rf-domain</b> .                                                                             |
| filter{offline online} | Optional. Specifies additional filters <ul style="list-style-type: none"><li>• offline – Optional. Displays global information for offline devices only</li><li>• online – Optional. Displays global information for online devices only</li></ul> |

```
show global device-list {filter rf-domain [<DOMAIN-NAME>/not <DOMAIN-NAME>]}
```

|                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| global device -list                                       | Displays global information for all network devices. Use the following keywords to specify additional filters: <b>offline</b> , <b>online</b> , and <b>rf-domain</b> .                                                                                                                                                                                                                                                                                                        |
| filter rf-domain<br>[<DOMAIN-NAME> <br>not <DOMAIN-NAME>] | Optional. Specifies additional filters <ul style="list-style-type: none"><li>• rf-domain – Optional. Displays global information for all devices in a specified RF Domain</li><li>• &lt;DOMAIN-NAME&gt; – Optional. Displays information for all devices within the domain identified by the &lt;DOMAIN-NAME&gt; keyword</li><li>• not &lt;DOMAIN-NAME&gt; – Optional. Displays information for all devices in domains not matching the &lt;DOMAIN-NAME&gt; keyword</li></ul> |

```
show global domain managers
```

|                        |                                                                         |
|------------------------|-------------------------------------------------------------------------|
| global domain managers | Displays global information for all RF Domains managers in the network. |
|------------------------|-------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config)#show global device-list filter rf-domain TechPubs
```

```

BY MAC HOST-NAME TYPE CLUSTER RF-DOMAIN ADOPTED-
ONLINE

00-15-70-81-74-2D rfs6000-81742D rfs6000 SiteConRFS6k TechPubs B4-
C7-99-6C-88-09 online
```



```

Total number of clients displayed: 1
nx9500-6C8809(config)#
nx9500-6C8809(config)#show global domain managers

```

```

APS CLIENTS

RF-DOMAIN MANAGER HOST-NAME

configuration default ? rf-domain manager 00-15-70-38-03-E7 not in
0 0 TechPubs 00-15-70-81-74-2D rfs6000-81742D

```

```

Total number of RF-domain displayed: 2
nx9500-6C8809(config)#

```

## gre

Displays layer 2 GRE (Generic Routing Encapsulation) tunnel traffic flow information

GRE is one of the available tunneling mechanisms which uses IP as the transport protocol and can be used for carrying many different passenger protocols. The tunnels behave as virtual point-to-point links that have two endpoints identified by the tunnel source and tunnel destination addresses at each endpoint.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show gre info {detail} {(on <DEVICE-NAME>)}
```

### Parameters

```
show gre info {detail} {(on <DEVICE-NAME>)}
```

|                  |                                                                                                                                                                                                                                                                                                                                                                 |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| gre info         | Displays GRE tunnel related information and stats.                                                                                                                                                                                                                                                                                                              |
| detail           | Optional. Displays GRE tunnel information in detail, such as tunnel state, tunnel's remote-end peer device's IP address, session ID of an operational tunnel, total number of packets received and transmitted through the tunnel, and the number of dropped packets during tunneled exchanges between access point and a peer at the remote end of the tunnel. |
| on <DEVICE-NAME> | Optional. Executes the command on a specified device <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the access point, controller, or service platform.</li> </ul>                                                                                                                                                           |

### Examples

```

nx9500-6C8809#show gre info
Gre Tunnel info:
Tunnel info not found
nx9500-6C8809#

```

## guest-registration

Displays information on the performance of clients using guest access permissions to obtain network resources within the WiNG network. The reporting timeline can be adjusted as needed, as can the RF Domain(s) and WLAN(s) used to filter and report guest client statistics.

### Supported in the following platforms:

- Service Platforms — NX 7510, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show guest-registration [age-range|backup-snapshots|browsers|client|devices|
gender|loyalty-app-status|notification-status|os|social|user-trends|visitors]
{on <DEVICE-NAME>}
show guest-registration backup-snapshots
show guest-registration [age-range|browsers|devices|gender|os|user-trends|
visitors] time [1-Day|1-Month|1-Week|2-Hours|30-Mins|5-Hours|all]
{(rfdomain <DOMAIN-NAME>/wlan <WLAN-NAME>)}
show guest-registration client [email|mac|member|mobile|name|time]
show guest-registration client [email <EMAIL-ADDRESS>|mac <MAC>|
member <MEMBER-ID>|mobile <MOBILE-NUMBER>|name <NAME>]
show guest-registration client time [1-Hour|10-Mins|15-Mins|2-Mins|30-Mins|
30-Secs|5-Mins] {(rfdomain <DOMAIN-NAME>/wlan <WLAN-NAME>)}
show guest-registration loyalty-app-status time [1-Day|1-Month|1-Week|2-Hours|
30-Mins|5-Hours|all] {rfdomain <RF-DOMAIN-NAME>/wlan <WLAN-NAME>}
show guest-registration notification-status
show guest-registration social time [1-Day|1-Month|1-Week|2-Hours|30-Mins|
5-Hours|all] {(facebook|rfdomain <DOMAIN-NAME>/wlan <WLAN-NAME>/google)}
```

### Parameters

```
show guest-registration backup-snapshots
```

|                    |                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| guest-registration | Displays guest registration statistics based on the parameters passed                                                                                                                                                                                                                                                                                                                                   |
| backup-snapshots   | Displays a list of periodically backed up snapshots of the database. By default, the system maintains a snapshot of the database on a daily basis.<br><br><b>Note:</b> Use the <b>service &gt; guest-registration &gt; backup [delete restore]</b> command to delete these snapshots and to restore deleted snapshots. For more information, see <a href="#">service</a> on page 647 (common commands). |

```
show guest-registration [age-range|browsers|devices|gender|os|user-trends|visitors]
time [1-Day|1-Month|1-Week|2-Hours|30-Mins|5-Hours|all] {(rfdomain <DOMAIN-NAME>/wlan
<WLAN-NAME>)}
```

|                    |                                                                                                                                                                                                                     |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| guest-registration | Displays guest registration statistics based on the parameters and time entered. Optionally, use the 'rfdomain' and/or 'wlan' keywords to view guest registration statistics for a specified RF Domain and/or WLAN. |
| age-range          | Displays the age ranges of logged guest users for a selected time period                                                                                                                                            |
| browser            | Displays the browsers used by guest users logged in within a selected time period                                                                                                                                   |
| devices            | Displays the device types used by guest users logged in within a selected time period                                                                                                                               |
| gender             | Displays the gender of guest users logged in within a selected time period                                                                                                                                          |
| os                 | Displays the OS (operating system) of devices logged in within a selected time period                                                                                                                               |

|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| user-trends                                                | Displays guest user login trends for a selected time period. It displays statistical data, such as number of new users, number of return users, and total of number users.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| visitors                                                   | Displays type of visitors logged in within a selected time period                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| time [1-Day 1-Month  1-Week  2-Hours  30-Mins 5-Hours all] | Displays guest registration statistics, for a specified time period. The stats displayed depends on the option selected in the previous step. Specify the time period using one of the following options: <ul style="list-style-type: none"> <li>• 1-Day – Displays previous day’s statistics</li> <li>• 1-Month – Displays previous month’s statistics</li> <li>• 1-Week – Displays previous week’s statistics</li> <li>• 2-Hours – Displays last 2 hours statistics</li> <li>• 30-Mins – Displays last 30 minutes statistics</li> <li>• 5-Hours – Displays last 5 hours statistics</li> <li>• all – Displays statistics from the day the database was created</li> </ul> |
| [rfdomain <DOMAIN-NAME  wlan <WLAN-NAME>]                  | Use the following options as additional filters: <ul style="list-style-type: none"> <li>• rfdomain &lt;DOMAIN-NAME&gt; – Optional. Displays guest registration statistics for a specified RF Domain. <ul style="list-style-type: none"> <li>• &lt;DOMAIN-NAME&gt; – Specify the RF Domain name.</li> </ul> </li> <li>• wlan &lt;WLAN-NAME&gt; – Optional. Displays guest registration statistics for a specified WLAN. <ul style="list-style-type: none"> <li>• &lt;WLAN-NAME&gt; – Specify the WLAN name.</li> </ul> </li> </ul>                                                                                                                                          |

```
show guest-registration client [email <EMAIL-ADDRESS>|mac <MAC>|member <MEMBER-ID>|
mobile <MOBILE-NUMBER>|name <NAME>]
```

|                       |                                                                                                                                                                                                                      |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| guest-registration    | Displays guest registration statistics based on the parameters and time entered. Optionally, use the 'rfdomain' and/or 'wlan' keywords to view guest registration statistics for a specified RF Domain and/or WLAN.  |
| client                | Displays statistical data for a specific client. Use the e-mail, mac, member, mobile, name to provide a match criteria.                                                                                              |
| email <EMAIL-ADDRESS> | Displays statistical data for the client with e-mail address matching the <EMAIL-ADDRESS> parameter <ul style="list-style-type: none"> <li>• &lt;EMAIL-ADDRESS&gt; – Specify the client’s e-mail address.</li> </ul> |
| mac <MAC>             | Displays statistical data for the client with MAC address matching the <MAC> parameter <ul style="list-style-type: none"> <li>• &lt;MAC&gt; – Specify the client’s MAC address</li> </ul>                            |
| member <MEMBER-ID>    | Displays statistical data for the client with member ID matching the <MEMBER-ID> parameter <ul style="list-style-type: none"> <li>• &lt;MEMBER-ID&gt; – Specify the client’s member ID.</li> </ul>                   |

|                        |                                                                                                                                                                                                                    |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mobile <MOBILE-NUMBER> | Displays statistical data for the client with mobile number matching the <MOBILE-NUMBER> parameter <ul style="list-style-type: none"> <li>• &lt;MOBILE-NUMBER&gt; - Specify the client's mobile number.</li> </ul> |
| name <NAME>            | Displays statistical data for the client with name matching the <NAME> parameter <ul style="list-style-type: none"> <li>• &lt;MOBILE-NUMBER&gt; - Specify the client's name.</li> </ul>                            |

```
show guest-registration client time [1-Hour|10-Mins|15-Mins|2-Mins|30-Mins|30-Secs|5-Mins]
{ (rfdomain <DOMAIN-NAME>/wlan <WLAN-NAME>) }
```

|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| guest-registration                                      | Displays guest registration statistics based on the parameters and time entered. Optionally, use the 'rfdomain' and/or 'wlan' keywords to view guest registration statistics for a specified RF Domain and/or WLAN.                                                                                                                                                                                                                                                                                                               |
| client                                                  | Displays statistical data for all clients logged in within a specified time period                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| time [1-Day 1-Month 1-Week 2-Hours 30-Mins 5-Hours all] | Use one of the following options to specify the time period <ul style="list-style-type: none"> <li>• 1-Day - Displays previous day's statistics</li> <li>• 1-Month - Displays previous month's statistics</li> <li>• 1-Week - Displays previous week's statistics</li> <li>• 2-Hours - Displays last 2 hours statistics</li> <li>• 30-Mins - Displays last 30 minutes statistics</li> <li>• 5-Hours - Displays last 5 hours statistics</li> <li>• all - Displays statistics from the day the database was created</li> </ul>      |
| [rfdomain <DOMAIN-NAME  wlan <WLAN-NAME>]               | Use the following options as additional filters: <ul style="list-style-type: none"> <li>• rfdomain &lt;DOMAIN-NAME&gt; - Optional. Displays guest registration statistics for a specified RF Domain. <ul style="list-style-type: none"> <li>• &lt;DOMAIN-NAME&gt; - Specify the RF Domain name.</li> </ul> </li> <li>• wlan &lt;WLAN-NAME&gt; - Optional. Displays guest registration statistics for a specified WLAN. <ul style="list-style-type: none"> <li>• &lt;WLAN-NAME&gt; - Specify the WLAN name.</li> </ul> </li> </ul> |

```
show guest-registration loyalty-app-status time [1-Day|1-Month|1-Week|2-Hours|
30-Mins|5-Hours|all] {rfdomain <RF-DOMAIN-NAME>/wlan <WLAN-NAME>}
```

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| guest-registration | Displays guest registration statistics based on the parameters and time entered                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| loyalty-app-status | Displays captive portal clients' Loyalty Application analytics, such as the number of guest clients with loyalty application detection enabled, associating with the captive portal's access point during a specified time period.<br>Loyalty application detection occurs on the access point to which the guest client is associated, allowing a retail administrator to assess whether a captive portal client is using specific retail (loyalty) applications in their captive portal. For more information on enabling loyalty application detection on a captive portal, see <a href="#">report-loyalty-application</a> (captive portal config mode). |

|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| time [1-Day 1-Month 1-Week 2-Hours 30-Mins 5-Hours all] | Use one of the following options to specify the time period <ul style="list-style-type: none"> <li>1-Day – Displays previous day’s captive portal clients’ Loyalty Application analytics</li> <li>1-Month – Displays previous month’s captive portal clients’ Loyalty Application analytics</li> <li>1-Week – Displays previous week’s captive portal clients’ Loyalty Application analytics</li> <li>2-Hours – Displays last 2 hours captive portal clients’ Loyalty Application analytics</li> <li>30-Mins – Displays last 30 minutes captive portal clients’ Loyalty Application analytics</li> <li>5-Hours – Displays last 5 hours captive portal clients’ Loyalty Application analytics</li> <li>all – Displays the entire Loyalty Application analytics, from the day the database was created</li> </ul> |
| {rfdomain <RF-DOMAIN-NAME>  wlan <WLAN-NAME>}           | Optional. Specifies the ‘rfdomain’ and/or ‘wlan’ to view guest registration statistics for a specified RF Domain and/or WLAN <ul style="list-style-type: none"> <li>rfdomain &lt;RF-DOMAIN-NAME&gt; – Displays Loyalty App analytics for a specified RF Domain <ul style="list-style-type: none"> <li>&lt;RF-DOMAIN-NAME&gt; – Specify the RF Domain name.</li> </ul> </li> <li>wlan &lt;WLAN-NAME&gt; – Displays Loyalty App analytics for a specified WLAN <ul style="list-style-type: none"> <li>&lt;WLAN-NAME&gt; – Specify the WLAN name.</li> </ul> </li> </ul>                                                                                                                                                                                                                                           |

`show guest-registration notification-status`

|                     |                                                                                                                                                                                                                     |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| guest-registration  | Displays guest registration statistics based on the parameters and time entered. Optionally, use the ‘rfdomain’ and/or ‘wlan’ keywords to view guest registration statistics for a specified RF Domain and/or WLAN. |
| notification-status | Displays guest registration notification status                                                                                                                                                                     |

`show guest-registration social time [1-Day|1-Month|1-Week|2-Hours|30-Mins|5-Hours|all] { (facebook|rfdomain <DOMAIN-NAME>|wlan <WLAN-NAME>|google) }`

|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| guest-registration social                               | Displays the social sites used by guests to register. Optionally, use the ‘rfdomain’ and/or ‘wlan’ keywords to view social site used by guests of a specified RF Domain and/or WLAN.                                                                                                                                                                                                                                                                                                                                                                   |
| time [1-Day 1-Month 1-Week 2-Hours 30-Mins 5-Hours all] | Displays social site statistics for a specified time period. Use one of the following time options: <ul style="list-style-type: none"> <li>1-Day – Displays previous day’s statistics</li> <li>1-Month – Displays previous month’s statistics</li> <li>1-Week – Displays previous week’s statistics</li> <li>2-Hours – Displays last 2 hours statistics</li> <li>30-Mins – Displays last 30 minutes statistics</li> <li>5-Hours – Displays last 5 hours statistics</li> <li>all – Displays statistics from the day the database was created</li> </ul> |
| facebook                                                | Displays guest users using Facebook to log in                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| rfdomain <DOMAIN-NAME>                                  | Displays guest users for a specific RF Domain <ul style="list-style-type: none"> <li>&lt;DOMAIN-NAME&gt; – Specify the RF Domain name.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                      |

|                  |                                                                                                                                         |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| wlan <WLAN-NAME> | Displays guest users for a specific WLAN <ul style="list-style-type: none"> <li>• &lt;WLAN-NAME&gt; - Specify the WLAN name.</li> </ul> |
| google           | Displays guest users using Google to log in                                                                                             |

### Examples

```
nx9500-6C8809#show guest-registration age-range time all
Timeline:
all
```

```

AGE RANGE COUNT

less_than_18 0 (0%)
18_to_24 1 (20%)
25_to_34 0 (0%)
35_to_44 1 (20%)
45_to_54 1 (20%)
55_to_64 2 (40%)
greater_than_64 0 (0%)

```

```
nx9500-6C8809#
nx9500-6C8809#show guest-registration browsers time 1-Day rfdomain Test-rfdomain-10
RF Domain: Test-rfdomain-10 Timeline: 1-
Day
```

```

BROWSER
COUNT

Safari 1 (50%)
Chrome 1 (50%)
```

```
nx9500-6C8809#
nx9500-6C8809#show guest-registration devices time 30-Mins wlan Test-ssid-9
WLAN: Test-ssid-9 Timeline: 30-Mins
```

```

DEVICE COUNT

Windows PC 1 (100%)
```

```
nx9500-6C8809#
nx9500-6C8809#show guest-registration gender time all wlan Test-ssid-10 rfdomain
Test-rfdomain-10
RF Domain: Test-rfdomain-10 WLAN: Test-ssid-10 Timeline: all
```

```

GENDER COUNT

Male 1 (50%)
Female 1 (50%)
Other 0 (0%)
```

```

nx9500-6C8809#
nx9500-6C8809#show guest-registration gender time all wlan Test-ssid-10 rfdomain
Test-rfdomain-9
%% No guests registered for specified inputs.

```

```

nx9500-6C8809#
nx9500-6C8809#show guest-registration os time 1-Day
Timeline: 1-Day

```

| OS        | COUNT    |
|-----------|----------|
| Windows 7 | 3 ( 30%) |
| Apple iOS | 3 ( 30%) |
| Macintosh | 3 ( 30%) |
| Windows 8 | 1 ( 10%) |

```

nx9500-6C8809#
nx9500-6C8809#show guest-registration social time 30-Mins
Timeline: 30-Mins

```

| SOCIAL | ONLINE   | TOTAL    |
|--------|----------|----------|
| google | 1 (100%) | 1 ( 10%) |
| Local  | 0 ( 0%)  | 9 ( 90%) |

```

nx9500-6C8809#
nx9500-6C8809#show guest-registration user-trends time all
Timeline: all

```

| SAMPLE RANGE            | NEW USERS | RETURN USERS | TOTAL |
|-------------------------|-----------|--------------|-------|
| 2014-2-16 - 2014-4-17   | 0 ( 0%)   | 0 ( 0%)      | 0     |
| 2014-4-17 - 2014-6-16   | 0 ( 0%)   | 0 ( 0%)      | 0     |
| 2014-6-16 - 2014-8-15   | 0 ( 0%)   | 0 ( 0%)      | 0     |
| 2014-8-15 - 2014-10-14  | 0 ( 0%)   | 0 ( 0%)      | 0     |
| 2014-10-14 - 2014-12-13 | 0 ( 0%)   | 0 ( 0%)      | 0     |
| 2014-12-13 - 2015-2-11  | 10 (100%) | 0 ( 0%)      | 10    |

```

nx9500-6C8809#
nx9500-6C8809#show guest-registration user-trends time 1-Day
Timeline: 1-Day

```

| SAMPLE RANGE  | NEW USERS | RETURN USERS | TOTAL |
|---------------|-----------|--------------|-------|
| 23:16 - 3:16  | 0 ( 0%)   | 0 ( 0%)      | 0     |
| 3:16 - 7:16   | 0 ( 0%)   | 0 ( 0%)      | 0     |
| 7:16 - 11:16  | 0 ( 0%)   | 0 ( 0%)      | 0     |
| 11:16 - 15:16 | 0 ( 0%)   | 0 ( 0%)      | 0     |
| 15:16 - 19:16 | 0 ( 0%)   | 0 ( 0%)      | 0     |
| 19:16 - 23:16 | 0 ( 0%)   | 0 ( 0%)      | 0     |

```

nx9500-6C8809#
nx9500-6C8809#show guest-registration visitors time 30-Mins
Timeline: 30-Mins

```

| VISITORS     | COUNT    |
|--------------|----------|
| New Users    | 7 ( 70%) |
| Return Users | 3 ( 30%) |

```
nx9500-6C8809#
nx9500-6C8809#show guest-registration client time 30-Mins email Guest_9@abc.com
```

```

ATTRIBUTE VALUE

city Brooklyn
wlan Test-ssid-10
name Guest_9
zip 11204
mobile 9131373709
gender female
llogintime 2015-01-20 19:11:14.001000
mobileok on
devtype Windows PC
createtime 2015-01-20 18:27:14.001000
email Guest_9@abc.com
mac 10-00-00-10-00-09
reg_type otp
rfd Test-rfdomain-10
agerange <18
group mac_reg_gr1
mid 1234100009
os Windows 7
exptime 2015-11-16 19:21:14.001000
browser Safari

```

```
nx9500-6C8809#
nx9500-6C8809#show guest-registration client time 30-Mins rfdomain Test-rfdomain-8
```

```

ATTRIBUTE VALUE

loggedin yes
wlan Test-ssid-8
name Guest_1
locale en_US
llogintime 2015-01-20 19:15:14
devtype Macintosh
exptime 2015-11-16 19:21:14
lname Guest_100000
source google
mac 10-00-00-10-00-01
email Guest_1@abc.com
id 657669862939196
reg_type device
fname Test-Guest_1
rfd Test-rfdomain-8
agerange 35-44
timezone 7
profilePic https://www.google.com/user_id/657669862939196/
os Macintosh
createtime 2015-01-20 18:45:14
group mac_reg_gr1
browser Chrome

city Santa Cruz
group mac_reg_gr1
name Guest_2
zip 95062
mobile 3700870747
mid 1234100001
llogintime 2015-01-20 19:18:14
mobileok on

```



```

devtype Apple iPad
exptime 2015-11-16 19:21:14
createtime 2015-01-20 19:11:14
mac 10-00-00-10-00-02
reg_type otp
rfd Test-rfdomain-8
agerange 55-64
wlan Test-ssid-8
os Apple iOS
email Guest_2@abc.com
browser Chrome

```

```

city Los Angeles
group mac_reg_gr1
name Guest_5
zip 90001
mobile 9129618672
mid 1234100005
llogintime 2015-01-20 19:20:14
devtype Macintosh
exptime 2015-11-16 19:21:14
createtime 2015-01-20 19:05:14
mac 10-00-00-10-00-05
reg_type device
rfd Test-rfdomain-8
agerange 18-24
wlan Test-ssid-8
os Macintosh
email Guest_5@abc.com
browser Chrome

```

```

nx9500-6C8809#
nx7500-112233#show guest-registration loyalty-app-status time all

```

```

Timeline: all

```

```

LOYALTY APP STATUS COUNT

Loyalty App Users 491 (49%)
Others 510 (51%)

```

```

nx7500-112233#

```

## interface

Displays configured system interfaces and their status

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```

show interface {<INTERFACE-NAME>|brief|counters|ge|me1|port-channel|pppoe1|
switchport|vlan|wwan1}
show interface {<INTERFACE-NAME>|brief|counters|ge <1-4>|me1|port-channel <1-2>|
pppoe1|switchport|vlan <1-4094>|wwan1} {on <DEVICE-NAME>}

```

## Parameters

show interface {<INTERFACE-NAME>/brief/counters/ge <1-4>/me1/port-channel <1-2>/pppoe1/switchport/vlan <1-4094>/wwan1} {on <DEVICE-NAME>}

|                    |                                                                                                                                                                                                                                                                                                                          |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| interfaces         | Optional. Displays system interface status based on the parameters passed                                                                                                                                                                                                                                                |
| <INTERFACE-NAME>   | Optional. Displays status of the interface specified by the <INTERFACE-NAME> parameter. Specify the interface name.                                                                                                                                                                                                      |
| brief              | Optional. Displays a brief summary of the interface status and configuration                                                                                                                                                                                                                                             |
| counters           | Optional. Displays interface Tx or Rx counters                                                                                                                                                                                                                                                                           |
| ge <1-4>           | Optional. Displays Gigabit Ethernet interface status and configuration <ul style="list-style-type: none"> <li>&lt;1-4&gt; - Select the Gigabit Ethernet interface index from 1 - 4.</li> </ul>                                                                                                                           |
| me1                | Optional. Displays Fast Ethernet interface status and configuration                                                                                                                                                                                                                                                      |
| port-channel <1-2> | Optional. Displays port channel interface status and configuration <ul style="list-style-type: none"> <li>&lt;1-2&gt; - Specify the port channel index from 1 - 2.</li> </ul>                                                                                                                                            |
| pppoe1             | Optional. Displays PPP over Ethernet interface status and configuration                                                                                                                                                                                                                                                  |
| switch port        | Optional. Displays layer 2 interface status                                                                                                                                                                                                                                                                              |
| vlan <1-4094>      | Optional. Displays VLAN interface status and configuration <ul style="list-style-type: none"> <li>&lt;1-4094&gt; - Specify the Switch Virtual Interface (SVI) VLAN ID from 1 - 4094.</li> </ul>                                                                                                                          |
| wwan1              | Optional. Displays Wireless WAN interface status, configuration, and counters                                                                                                                                                                                                                                            |
| on <DEVICE-NAME>   | The following keywords are common to all of the above interfaces: <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; - Optional. Displays interface related information on a specified device</li> <li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

## Examples

```
nx9500-6C8809(config)#show interface switchport
```

```

INTERFACE STATUS MODE VLAN(S)

ge1 UP access 1
ge2 DOWN access 1

```

A '\*' next to the VLAN ID indicates the native vlan for that trunk port

```
nx9500-6C8809(config)#
```

```
nx9500-6C8809(config)#show interface vlan 1
```

```
Interface vlan1 is UP
```

```
Hardware-type: vlan, Mode: Layer 3, Address: B4-C7-99-6C-88-09
```

```
Index: 5, Metric: 1, MTU: 1500
```

```
IP-Address: 192.168.13.13/24
```

```
input packets 4623946, bytes 568905032, dropped 0, multicast packets 0
```

```
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
```

```
output packets 458235, bytes 90317187, dropped 0
```

```
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
```

```
collisions 0
```

```
IPv6 mode is disabled
```

```
nx9500-6C8809(config)#
```

```
nx9500-6C8809(config)#show interface ge 1
```

```
Interface ge1 is UP
```

```
Hardware-type: ethernet, Mode: Layer 2, Address: 00-1E-67-4B-BF-BC
```

```
Index: 2001, Metric: 1, MTU: 1500
Speed: Admin Auto, Operational 1G, Maximum 1G
Duplex: Admin Auto, Operational Full
Active-medium: n/a
Input packets 2326745, bytes 348775278, dropped 0
Received 2326745 unicasts, 4367 broadcasts, 1219173 multicasts
Input errors 0, runts 0, giants 0
CRC 0, frame 0, fragment 0, jabber 0
Output packets 1080901, bytes 244595966, dropped 0
Sent 1080901 unicasts, 392 broadcasts, 132573 multicasts
Output errors 0, collisions 0, late collisions 0
Excessive collisions 0
```

```
nx9500-6C8809(config)#
nx9500-6C8809(config)#show interface counters
```

```

```

| INTF<br>BYTES           | MAC<br>TX-DROP         | RX-PKTS | RX-BYTES  | RX-DROP | TX-PKTS | TX- |
|-------------------------|------------------------|---------|-----------|---------|---------|-----|
| vlan1<br>90924957       | B4-C7-99-6C-88-09<br>0 | 2571193 | 341672167 | 0       | 625888  |     |
| ge1<br>244588229        | 00-1E-67-4B-BF-BC<br>0 | 2326629 | 348759017 | 0       | 1080855 |     |
| ge2<br>0                | 00-1E-67-4B-BF-BD<br>0 | 0       | 0         | 0       | 0       |     |
| port..nell<br>244588673 | 00-1E-67-4B-BF-BC<br>0 | 2326631 | 348759243 | 0       | 1080857 |     |

```

```

```
nx9500-6C8809(config)#
```

### *iot-device-type-imagotag*

Displays the configuration of ESL communicator on a specified AP or on all APs within an RF Domain.

#### **Supported in the following platforms:**

- Access Points — AP 8432
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### **Syntax**

```
show iot-device-type-imagotag status {on <DEVICE-OR-DOMAIN-NAME>}
```

#### **Parameters**

```
show iot-device-type-imagotag status {on <DEVICE-OR-DOMAIN-NAME>}
```

|                                 |                                                                                                                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| iot-device-type-imagotag status | Displays Imagotags ESL communicator configuration at device or domain level status                                                                                                               |
| on <DEVICE-NAME>                | Optional. Displays configuration on a specified device or RF Domain <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; - Specify the name of the AP or RF Domain.</li> </ul> |

#### **Example**

```
ap8432-9A5BD8#show iot-device-type-imagotag status
```

```

```



```
Imagotag Policy Dongle-Status AP-ID Channel Window Payload Max Output SSL FCC-Mode
ACS
```

```
Size Size Power
```

```

Enabled Disconnected 25982 7 14 32 A Enabled Enabled
Enabled
```

```
Enabled Enabled Connected 45290 10 14 32 A Enabled Enabled
Enabled
```

```

Total devices: 2
```

```
ap8432-9A5BD8#
```

```
ap8432-9A5BD8#show iot-device-type-imagotag status on ap8432-9A5BD8
```

```

Imagotag Policy Dongle-Status AP-ID Channel Window Payload Max Output SSL FCC-Mode
ACS
```

```
Size Size Power
```

```

Enabled Connected 45290 10 14 32 A Enabled Enabled
Enabled
```

```

Total devices: 1
```

```
ap8432-9A5BD8#
```

```
ap8432-9A5BD8#show iot-device-type-imagotag status on default
```

```

Imagotag Policy Dongle-Status AP-ID Channel Window Payload Max Output SSL FCC-Mode
ACS
```

```
Size Size Power
```

```

Enabled Disconnected 25982 7 14 32 A Enabled Enabled
Enabled
```

```
Enabled Enabled Connected 45290 10 14 32 A Enabled Enabled
Enabled
```

```

Total devices: 2
```

```
ap8432-9A5BD8#
```

```
ap8432-9A5BD8#show iot-device-type-imagotag status on default/ap8432-9A5BD8
```

```

Imagotag Policy Dongle-Status AP-ID Channel Window Payload Max Output SSL FCC-Mode
ACS
```

```
Size Size Power
```

```

Enabled Connected 45290 10 14 32 A Enabled Enabled
Enabled
```

```

Total devices: 1
```

```
ap8432-9A5BD8#
```

*ip*

Displays IP related information

## Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
show ip [arp|bgp|ddns|default-gateways|dhcp|dhcp-vendor-options|domain-name|
extcommunity-list|igmp|interface|name-server|nat|ospf|route|routing]
show ip arp {<VLAN-NAME>} {(on <DEVICE-NAME>)}
show ip bgp {<IP>|<IP/M>|community|community-list|filter-list|neighbors|
on|paths|prefix-list|regexp|route-map|state|summary}
show ip ddns bindings {on <DEVICE-NAME>}
show ip dhcp [binding|networks|status]
show ip dhcp binding {manual} {(on <DEVICE-NAME>)}
show ip dhcp [networks|status] {on <DEVICE-NAME>}
show ip [default-gateways|dhcp-vendor-options|domain-name|name-server|routing] {on <DEVICE-
NAME>}
show ip extcommunity-list [<1-500>|<NAME>]
show ip igmp snooping [mrouter|querier|vlan]
show ip igmp snooping [mrouter|querier] vlan <1-4095> {on <DEVICE-NAME>}
show ip igmp snooping vlan <1-4095> {<IP>} {(on <DEVICE-NAME>)}
show ip interface {<INTERFACE-NAME>|brief|on}
show ip interface {<INTERFACE-NAME>|brief} {(on <DEVICE-NAME>)}
show ip nat translations verbose {on <DEVICE-NAME>}
show ip route {<INTERFACE-NAME>|ge|me1|on|port-channel|pppoe1|vlan|wwan1}
show ip route {<INTERFACE-NAME>|ge <1-4>|me1|port-channel <1-2>|vlan <1-4094>|
pppoe1|wwan1} {(on <DEVICE-NAME>)}
show ip ospf {border-router|interface|neighbor|on|route|state}
show ip ospf {border-router|neighbor|route|on|state} {on <DEVICE-NAME>}
show ip ospf {interface} {vlan|on}
show ip ospf {interface} {vlan <1-4094>} {(on <DEVICE-NAME>)}
```



### Note

The **show > ip > ospf** command is also available under the 'profile' and 'device' modes.

## Parameters

```
show ip arp {<VLAN-NAME>} {(on <DEVICE-NAME>)}
```

|                  |                                                                                                                                                                                                                                                                                                                                 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip arp           | Displays ARP (Address Resolution Protocol) mappings                                                                                                                                                                                                                                                                             |
| <VLAN-NAME>      | Optional. Displays ARP mapping on a specified VLAN. Specify the VLAN name.                                                                                                                                                                                                                                                      |
| on <DEVICE-NAME> | The following keyword is recursive and common to the 'vlan-name' parameter: <ul style="list-style-type: none"><li>• on &lt;DEVICE-NAME&gt; - Optional. Displays ARP configuration details on a specified device</li><li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li></ul> |

```
show ip bgp {<IP>|<IP/M>|community|community-list|filter-list|neighbors|on|
paths|prefix-list|regexp|route-map|state|summary}
```

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip bgp                         | Displays BGP routing table statistics based on the match criteria specified here. Routes matching the specified criteria are filtered. Use available options to filter the information displayed.<br>This command is applicable to the RFS 4000 and NX 95XX model devices.                                                                                                                                                                                                                                                                                                                                                                                        |
| <IP>                           | Optional. Filters routes matching the specified IP address                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <IP/M>                         | Optional. Filters routes matching the specified network                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| community                      | Optional. Filters routes based on the community attribute specified. The options are: <ul style="list-style-type: none"> <li>• AA:NN – Filters routes based on the community number (AA: is the autonomous system number (ASN), NN: is the community number within the specified ASN)</li> <li>• local-as – Filters routes carrying the local-as attribute (these routes are not sent outside the local AS)</li> <li>• no-advertise – Filters routes carrying the no-advertise attribute (these routes are not advertised to any peers)</li> <li>• no-export – Filters routes carrying no-export attribute (these routes are not exported to next AS)</li> </ul>  |
| community-list                 | Optional. Displays routes that are members of communities included in the specified BGP community-list <ul style="list-style-type: none"> <li>• &lt;1-500&gt; – Specify the community-list number.</li> <li>• &lt;WORD&gt; – Specify the community-list name.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                          |
| filter-list                    | Optional. Filters routes having AS-path matching the specified AS-path access list. Specify the AS-path ACL name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| neighbors                      | Optional. Displays BGP neighbor details. Specify the IP address, to view a specific neighbor details. Use one of the following options to filter information: <ul style="list-style-type: none"> <li>• advertised-routes – Displays route information for routes advertised to the selected neighbor device</li> <li>• received-routes – Displays route information for routes received from the selected neighbor device</li> <li>• routes – Displays the route information for routes learned from the selected neighbor device</li> </ul> <p>If no neighbor IP address is specified, the system displays all neighbor-related routes on the logged device.</p> |
| on <DEVICE-NAME>               | Optional. Displays BGP routing table statistics on a specified device <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| paths                          | Optional. Displays BGP path details                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| prefix-list <PREFIX-LIST-NAME> | Optional. Displays routes conforming to the specified prefix-list <ul style="list-style-type: none"> <li>• &lt;PREFIX-LIST-NAME&gt; – Specify the prefix list name.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| regexp <LINE>                  | Optional. Displays routes matching the specified AS path regular expression <ul style="list-style-type: none"> <li>• &lt;LINE&gt; – Specify the regular expression.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| route-map <ROUTE-MAP-NAME>     | Optional. Displays routes matching the specified route map <ul style="list-style-type: none"> <li>• &lt;ROUTE-MAP-NAME&gt; – Specify the route map name.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

```
show ip ddns bindings {on <DEVICE-NAME>}
```

|                             |                                                                                                                                                                                                                                                                          |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip ddns                     | Displays DDNS (Dynamic Domain Name Server) configuration details                                                                                                                                                                                                         |
| bindings {on <DEVICE-NAME>} | Displays DDNS address bindings <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; - Optional. Displays address bindings on a specified device</li> <li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
show ip dhcp [networks|status] {on <DEVICE-NAME>}
```

|                  |                                                                                                                                                                                                                                                                                                                            |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip dhcp          | Displays the DHCP server configuration details                                                                                                                                                                                                                                                                             |
| networks         | Displays DHCP server network details                                                                                                                                                                                                                                                                                       |
| status           | Displays DHCP server status                                                                                                                                                                                                                                                                                                |
| on <DEVICE-NAME> | The following keyword is common to all of the above parameters: <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; - Optional. Displays server status and network details on a specified device</li> <li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
show ip dhcp binding {manual} {(on <DEVICE-NAME>)}
```

|                  |                                                                                                                                                                                                                                                                                                                         |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip dhcp          | Displays the DHCP server configuration details                                                                                                                                                                                                                                                                          |
| bindings         | Displays DHCP address bindings                                                                                                                                                                                                                                                                                          |
| manual           | Displays static DHCP address bindings                                                                                                                                                                                                                                                                                   |
| on <DEVICE-NAME> | The following keyword is recursive and common to the 'manual' parameter: <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; - Optional. Displays DHCP address bindings on a specified device</li> <li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
show ip extcommunity-list [<1-500>|<NAME>]
```

|                                       |                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip extcommunity-list [<1-500> <NAME>] | Displays the specified extended community list details <ul style="list-style-type: none"> <li>&lt;1-500&gt; - Specify the extended community number from 1 - 500.</li> <li>&lt;NAME&gt; - Specify the extended community name.</li> </ul> <p>This command is applicable to the RFS 4000 and NX 95XX model devices.</p> |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
show ip [default-gateways|dhcp-vendor-options|domain-name|name-server|routing] {on <DEVICE-NAME>}
```

|                        |                                                                                                                                  |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| ip default-gateways    | Displays all learnt default gateways                                                                                             |
| ip dhcp-vendor-options | Displays DHCP 43 parameters received from the DHCP server. This output includes the interface from which the option was learned. |
| ip domain-name         | Displays the DNS default domain                                                                                                  |
| ip name-server         | Displays the DNS name server details                                                                                             |

|                  |                                                                                                                                                                                                                                                                                                                                                    |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip routing       | Displays routing status                                                                                                                                                                                                                                                                                                                            |
| on <DEVICE-NAME> | The following keywords are common to all of the above parameters: <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; - Optional. Displays IP related information, based on the parameters passed, on a specified device</li> <li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
show ip igmp snooping [mrouter|querier] vlan <1-4095> {on <DEVICE-NAME>}
```

|                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip igmp snooping                 | Displays the IGMP snooping configuration                                                                                                                                                                                                                                                                                                                                                                                                     |
| mrouter                          | Displays the IGMP snooping multicast router (mrouter) configuration                                                                                                                                                                                                                                                                                                                                                                          |
| querier                          | Displays the IGMP snooping multicast querier configuration                                                                                                                                                                                                                                                                                                                                                                                   |
| vlan <1-4095> {on <DEVICE-NAME>} | Displays the IGMP snooping multicast router configuration for a VLAN <ul style="list-style-type: none"> <li>&lt;1-4095&gt; - Specify the VLAN ID from 1 - 4095.</li> <li>on &lt;DEVICE-NAME&gt; - Optional. Displays the IGMP snooping mrouter configuration on a specified device <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> </li> </ul> |

```
show ip igmp snooping vlan <1-4095> {<IP>} {(on <DEVICE-NAME>)}
```

|                  |                                                                                                                                                                                                                                                                                                                     |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip igmp snooping | Displays the IGMP snooping configuration                                                                                                                                                                                                                                                                            |
| vlan <1-4095>    | Displays the VLAN IGMP snooping configuration <ul style="list-style-type: none"> <li>&lt;1-4095&gt; - Specify the VLAN ID from 1 - 4095.</li> </ul>                                                                                                                                                                 |
| <IP>             | Optional. Specifies the multicast group IP address                                                                                                                                                                                                                                                                  |
| on <DEVICE-NAME> | The following keyword is recursive and common to the 'ip' parameter: <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; - Optional. Displays configuration details on a specified device</li> <li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
show ip interface {<INTERFACE-NAME>/brief} {(on <DEVICE-NAME>)}
```

|                  |                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip interface     | Displays an administrative and operational status of all layer 3 interfaces or a specified layer 3 interface                                                                                                                                                                                                                                                                         |
| <INTERFACE-NAME> | Displays a specified interface status. Specify the interface name.                                                                                                                                                                                                                                                                                                                   |
| brief            | Displays a brief summary of all interface status and configuration                                                                                                                                                                                                                                                                                                                   |
| on <DEVICE-NAME> | The following keyword is recursive and common to the 'interface-name' and 'brief' parameters: <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; - Optional. Displays interface status and summary, based on the parameters passed, on a specified device</li> <li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
show ip nat translations verbose {on <DEVICE-NAME>}
```



|                     |                                                                                                                                                                                                                                                                              |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip nat translations | Displays NAT (Network Address Translation) translations                                                                                                                                                                                                                      |
| verbose             | Displays detailed NAT translations <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; – Optional. Displays NAT translations on a specified device</li> <li>&lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
show ip route {<INTERFACE-NAME>/ge <1-4>/me1/port-channel <1-2>/vlan <1-4094>/pppoe1/
wwan1}
{(on <DEVICE-NAME>)}
```

|                    |                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip route           | Displays route table details. The route tables use flags to distinguish between routes. The different flags are: <ul style="list-style-type: none"> <li>C – Connected</li> <li>G – Gateway</li> <li>O – OSPF route</li> <li>S – Static route</li> </ul> <p><b>Note:</b> Flags 'S' and 'O' identify static learned routes and dynamic learned routes respectively.</p> |
| <INTERFACE-NAME>   | Optional. Displays route table details for a specified interface. Specify the interface name                                                                                                                                                                                                                                                                          |
| ge <1-4>           | Displays GigabitEthernet interface route table details <ul style="list-style-type: none"> <li>&lt;1-4&gt; – Specify the GigabitEthernet interface index from 1 - 4.</li> </ul>                                                                                                                                                                                        |
| me1                | Displays FastEthernet interface route table details                                                                                                                                                                                                                                                                                                                   |
| port-channel <1-2> | Displays port channel interface route table details. Specify the port channel index from 1 - 2.                                                                                                                                                                                                                                                                       |
| vlan <1-4095>      | Displays VLAN interface route table details. Select the VLAN interface ID from 1 - 4094.                                                                                                                                                                                                                                                                              |
| pppoe1             | Displays PPPoE interface route table details                                                                                                                                                                                                                                                                                                                          |
| wwan1              | Displays Wireless WAN route table details                                                                                                                                                                                                                                                                                                                             |
| on <DEVICE-NAME>   | The following keywords are recursive and common to all of the above parameters: <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; – Displays route table details, based on the parameters passed, on a specified device</li> <li>&lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul>                   |

```
show ip ospf {border-router/interface/neighbor/route/on/state}{on <DEVICE-NAME>}
```

|                                                  |                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip ospf                                          | Displays overall OSPF information                                                                                                                                                                                                                                                                                                                             |
| border-router                                    | Optional. Displays details of all the border routers connected                                                                                                                                                                                                                                                                                                |
| interface {on  vlan <1-4094>} {on <DEVICE-NAME>} | Optional. Displays details of all the interfaces with OSPF enabled <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; – Optional. Displays specified device details</li> <li>vlan &lt;1-4094&gt; – Displays VLAN interface details</li> <li>&lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul> |
| neighbor                                         | Optional. Displays an OSPF neighbors list                                                                                                                                                                                                                                                                                                                     |
| route                                            | Optional. Displays OFPS routes information                                                                                                                                                                                                                                                                                                                    |

|                  |                                                                                                                                                                                                                                                                                                                                                                    |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| state            | Optional. Displays an OSPF process state                                                                                                                                                                                                                                                                                                                           |
| on <DEVICE-NAME> | The following keywords are recursive and common to all of the above parameters: <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; - Optional. Displays overall OSPF information, based on the parameters passed, on a specified device</li> <li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

## Examples

```
nx9500-6C8809(config)#show ip arp
```

| IP            | MAC               | INTERFACE | TYPE    |
|---------------|-------------------|-----------|---------|
| 192.168.13.10 | 00-02-B3-28-D1-55 | vlan1     | dynamic |
| 192.168.13.13 | B4-C7-99-6C-88-09 | vlan1     | dynamic |
| 192.168.13.2  | 00-0F-8F-19-BA-4C | vlan1     | dynamic |

```
nx9500-6C8809(config)#
```

```
nx9500-6C8809(config)#show ip interface brief
```

| INTERFACE | IP-ADDRESS/MASK  | TYPE    | STATUS | PROTOCOL |
|-----------|------------------|---------|--------|----------|
| me1       | unassigned       | n/a     | UP     | down     |
| vlan1     | 192.168.13.24/24 | primary | UP     | up       |

```
nx9500-6C8809(config)#
```

```
nx9500-6C8809(config)#show ip route
```

| DESTINATION     | GATEWAY      | FLAGS | INTERFACE | METRIC | DISTANCE |
|-----------------|--------------|-------|-----------|--------|----------|
| default         | 192.168.13.2 | S     | vlan1     | 0      | 1        |
| 192.168.13.0/24 | 0.0.0.0      | C     | vlan1     | 0      | 0        |

Flags: C - Connected G - Gateway O - OSPF B - BGP S - Static

Gateway: N - Normalized Gateway Address

```
nx9500-6C8809(config)#
```

```
nx9500-6C8809(config)#show ip route port-channel 1
```

| DESTINATION     | GATEWAY      | FLAGS | INTERFACE | METRIC | DISTANCE |
|-----------------|--------------|-------|-----------|--------|----------|
| 192.168.0.0/24  | direct       | C     | me1       | 0      | 0        |
| 172.18.0.0/24   | direct       | C     | vlan1     | 0      | 0        |
| 10.2.0.0/24     | 172.18.0.1   | S     | vlan1     | 0      | 1        |
| default         | 192.168.13.2 | S     | vlan192   | 0      | 1        |
| 192.168.13.0/24 | direct       | C     | vlan192   | 0      | 0        |

Flags: C - Connected G - Gateway O - OSPF B - BGP S - Static

Gateway: N - Normalized Gateway Address

```
nx9500-6C8809(config)#
```

```
nx9500-6C8809(config)#show ip routing on rfs6000-81742D
```

IP routing is enabled.

```
nx9500-6C8809(config)#
```

```
nx9500-6C8809(config)#show ip dhcp status
```

State of DHCP server: not-running

```
nx9500-6C8809(config)#
```

```
nx9500-6C8809(config)#show ip ospf state
```

Maximum number of OSPF routes allowed: 9216

Number of OSPF routes received: 0

Ignore-count allowed: 5, current ignore-count: 0

Ignore-time 60 seconds, reset-time 360 seconds

Current OSPF process state: Running

```
nx9500-6C8809(config)#
```

## ip-access-list-stats

Displays IP access list statistics



### Note

This command is not available in the USER EXEC Mode.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show ip-access-list-stats {<IP-ACCESS-LIST-NAME>/detail/on}
show ip-access-list stats {<IP-ACCESS-LIST-NAME>/detail <IP-ACCESS-LIST-NAME>}
{(on <DEVICE-NAME>)}
```

### Parameters

```
show ip-access-list stats {<IP-ACCESS-LIST-NAME>/detail <IP-ACCESS-LIST-NAME>}
{(on <DEVICE-NAME>)}
```

|                              |                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip-access-list-stats         | Displays IP access list statistics                                                                                                                                                                                                                                                                                                                           |
| <IP-ACCESS-LIST-NAME>        | Optional. Displays statistics for a specified IP access list. Specify the IP access list name.                                                                                                                                                                                                                                                               |
| detail <IP-ACCESS-LIST-NAME> | Optional. Displays detailed statistics for a specified IP access list. Specify the IP access list name.                                                                                                                                                                                                                                                      |
| on <DEVICE-NAME>             | The following keyword is recursive and common to the 'IP-ACCESS-LIST-NAME' parameter: <ul style="list-style-type: none"><li>• on &lt;DEVICE-NAME&gt; - Optional. Displays all or a specified IP access list statistics on a specified device</li><li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li></ul> |

### Examples

```
nx9500-6C8809(config)#show ip-access-list stats
IP Access-list: # Restrict Management ACL #
 permit tcp any any eq ftp rule-precedence 1 Hitcount: 0
 permit tcp any any eq www rule-precedence 2 Hitcount: 4
 permit tcp any any eq ssh rule-precedence 3 Hitcount: 448
 permit tcp any any eq https rule-precedence 4 Hitcount: 0
 permit udp any any eq snmp rule-precedence 5 Hitcount: 0
 permit tcp any any eq telnet rule-precedence 6 Hitcount: 4
nx9500-6C8809(config)#
```

The following example displays the 'auto-tunnel-acl' IP ACL configuration:

```
rfs4000-1B3596(config)#ip access-list auto-tunnel-acl
rfs4000-1B3596(config-ip-acl-auto-tunnel-acl)#show context
ip access-list auto-tunnel-acl
 permit ip host 200.200.200.99 30.30.30.1/24 rule-precedence 2
 permit ip host 200.200.200.99 any rule-precedence 3
rfs4000-1B3596(config-ip-acl-auto-tunnel-acl)#
```

The following example displays the statistics for the 'auto-tunnel-acl' ACL:

```
rfs4000-1B3596#show ip-access-list stats
IP Access-list: auto-tunnel-acl
 permit ip host 200.200.200.99 30.30.30.1/24 rule-precedence 2 Hitcount: 0
 permit ip host 200.200.200.99 any rule-precedence 3 Hitcount: 0

rfs4000-1B3596#
```

## ipv6

Displays IPv6 related information and statistical data

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show ipv6 [default-gateways|delegated-prefix|dhcp|hop-limit|interface|mld|name-server|
neighbors|route]
show ipv6 [default-gateways|delegated-prefix|hop-limit|name-server] {on <DEVICE-NAME>}
show ipv6 dhcp [client received-options|relay status|status] {on <DEVICE-NAME>}
show ipv6 interface {<IF-NAME>/brief} {(on <DEVICE-NAME>)}
show ipv6 mld snooping [mrouter vlan <1-4095>|querier vlan <1-4095>|vlan <1-4095>]
{on <DEVICE-NAME>}
show ipv6 neighbors <VLAN-NAME> {(on <DEVICE-NAME>)}
show ipv6 route {<IF-NAME>/ge <1-X>/me1/port-channel <1-2>/pppoe1/serial <1-4>/
t1e1 <1-4> <1-1>/up/vlan <1-4095>/wwan1/xge} {(on <DEVICE-NAME>)}
```

### Parameters

```
show ipv6 [default-gateways|delegated-prefix|hop-limit|name-server] {on <DEVICE-NAME>}
```

|                  |                                                                                                                                                                                                                                                                                                                                                              |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ipv6             | Displays IPv6 related information and statistical data                                                                                                                                                                                                                                                                                                       |
| default-gateways | Displays all learnt default gateways                                                                                                                                                                                                                                                                                                                         |
| delegated-prefix | Displays prefix delegation information                                                                                                                                                                                                                                                                                                                       |
| hop-limit        | Displays the configured IPv6 hop count value                                                                                                                                                                                                                                                                                                                 |
| name-server      | Displays DNS name servers                                                                                                                                                                                                                                                                                                                                    |
| on <DEVICE-NAME> | This parameter is common to all of the above keywords. <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; - Optional. Displays the specified information on a device (access point, wireless controller, or service platform)</li> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
show ipv6 dhcp [client received-options|relay status|status] {on <DEVICE-NAME>}
```

|                         |                                                        |
|-------------------------|--------------------------------------------------------|
| ipv6                    | Displays IPv6 related information and statistical data |
| dhcp                    | Displays DHCPv6 related information                    |
| client received-options | Displays DHCP options received from clients            |
| relay status            | Displays the DHCPv6 relay agent's running status       |

|                  |                                                                                                                                                                                                                                                                                                                                                          |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| status           | Displays the DHCPv6 stateless server daemon's status. In case the DHCPv6 server is up and running, it also displays interface names.                                                                                                                                                                                                                     |
| on <DEVICE-NAME> | This parameter is common to all of the above keywords. <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; - Optional. Displays the specified information on a device (access point, wireless controller, or service platform)</li> <li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
show ipv6 interface {<IF-NAME>|brief} {(on <DEVICE-NAME>)}
```

|                             |                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ipv6                        | Displays IPv6 related information and statistical data                                                                                                                                                                                                                                                                                                   |
| interface {<IF-NAME> brief} | Displays IPv6 status and configuration on a specified interface related information <ul style="list-style-type: none"> <li>&lt;IF-NAME&gt; - Optional. Specify the interface name. <ul style="list-style-type: none"> <li>brief - Optional. Displays a brief summary of IPv6 status and configuration on the specified interface</li> </ul> </li> </ul>  |
| on <DEVICE-NAME>            | This parameter is common to all of the above keywords. <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; - Optional. Displays the specified information on a device (access point, wireless controller, or service platform)</li> <li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
show ipv6 mld snooping [mrouter vlan <1-4095>|querier vlan <1-4095>|vlan <1-4095>]
{on <DEVICE-NAME>}
```

|                       |                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ipv6                  | Displays IPv6 related information and statistical data                                                                                                                                                                                                                                                                                                   |
| mld snooping          | Displays MLD (Multicast Listener Discovery Protocol) snooping related information                                                                                                                                                                                                                                                                        |
| mrouter vlan <1-4095> | Displays IPv6 multicast router information on the specified VLAN                                                                                                                                                                                                                                                                                         |
| querier vlan <1-4095> | Displays IPv6 multicast querier information on the specified VLAN                                                                                                                                                                                                                                                                                        |
| vlan <1-4095>         | Displays MLD snooping related information on the specified VLAN                                                                                                                                                                                                                                                                                          |
| on <DEVICE-NAME>      | This parameter is common to all of the above keywords. <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; - Optional. Displays the specified information on a device (access point, wireless controller, or service platform)</li> <li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
show ipv6 neighbors <VLAN-NAME> {(on <DEVICE-NAME>)}
```

|                       |                                                                                                                                                                                                                                                                |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ipv6                  | Displays IPv6 related information and statistical data                                                                                                                                                                                                         |
| neighbors <VLAN-NAME> | Displays IPv6 neighbors on the specified VLAN                                                                                                                                                                                                                  |
| on <DEVICE-NAME>      | Optional. Displays IPv6 neighbors on a specified device (access point, wireless controller, or service platform) <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
show ipv6 route {<IF-NAME>|ge <1-X>|me1|port-channel <1-2>|pppoe1|serial <1-4>|
t1e1 <1-4> <1-1>|up|vlan <1-4095>|wwan1|xge} {(on <DEVICE-NAME>)}
```

|                    |                                                                                                                                                                                                                                                                                                                                                          |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ipv6               | Displays IPv6 related information and statistical data                                                                                                                                                                                                                                                                                                   |
| route              | Displays IPv6 route table                                                                                                                                                                                                                                                                                                                                |
| <IF-NAME>          | Optional. Displays IPv6 route table for the interface identified by the <IF-NAME> keyword                                                                                                                                                                                                                                                                |
| ge <1-X>           | Optional. Displays IPv6 route table for the selected GigabitEthernet interface                                                                                                                                                                                                                                                                           |
| me1                | Optional. Displays IPv6 route table for the FastEthernet interface                                                                                                                                                                                                                                                                                       |
| port-channel <1-2> | Optional. Displays IPv6 route table for the selected port-channel interface                                                                                                                                                                                                                                                                              |
| pppoe1             | Optional. Displays IPv6 route table for the PPP over Ethernet interface                                                                                                                                                                                                                                                                                  |
| vlan <1-4095>      | Optional. Displays IPv6 route table for the selected VLAN interface                                                                                                                                                                                                                                                                                      |
| up                 | Optional. Displays IPv6 route table for the WAN Ethernet interface                                                                                                                                                                                                                                                                                       |
| wwan               | Optional. Displays IPv6 route table for the wireless WAN interface                                                                                                                                                                                                                                                                                       |
| xge <1-4>          | Optional. Displays IPv6 route table for the selected TenGigabitEthernet interface                                                                                                                                                                                                                                                                        |
| on <DEVICE-NAME>   | This parameter is common to all of the above keywords. <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; - Optional. Displays the specified information on a device (access point, wireless controller, or service platform)</li> <li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

## Examples

```
rfs4000-229D58(config)#show ipv6 route
```

```

```

| DESTINATION    | GATEWAY     | FLAGS | INTERFACE |
|----------------|-------------|-------|-----------|
| 2000:abcd::/64 | fe80::300:1 | S     | vlan300   |
| default        | fe80::11:1  | R     | vlan11    |
| 4444:1111::/64 | direct      | C     | vlan1     |

```

```

```
Flags: C - Connected G - Gateway S - Static R - IPv6-RA
```

```
rfs4000-229D58(config)#
```

```
rfs4000-229D58#show ipv6 default-gateways
```

```

```

|                              |                               |
|------------------------------|-------------------------------|
| Source: IPv6-RA              | Gateway-address : fe80::100:1 |
| Preference: medium           | Status : not-monitored        |
| Installed : NO               | Interface : vlan100           |
| Remaining Lifetime: 1471 sec |                               |

```

```

|                              |                             |
|------------------------------|-----------------------------|
| Source: IPv6-RA              | Gateway-address : fe80::1:2 |
| Preference: low              | Status : not-monitored      |
| Installed : NO               | Interface : vlan1           |
| Remaining Lifetime: 1488 sec |                             |

```

```

|                             |                                |
|-----------------------------|--------------------------------|
| Source: Static-Route        | Gateway-address : fe80::2000:1 |
| Preference: NA              | Status : unreachable           |
| Installed : NO              | Interface : vlan2000           |
| Remaining Lifetime: forever |                                |

```

```

|                              |                              |
|------------------------------|------------------------------|
| Source: IPv6-RA              | Gateway-address : fe80::11:1 |
| Preference: high             | Status : reachable           |
| Installed : YES              | Interface : vlan11           |
| Remaining Lifetime: 1471 sec |                              |

-----  
rfs4000-229D58#

### ipv6-access-list

Displays IPv6 access list related information and statistics



#### Note

This command is not available in the USER EXEC Mode.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
show ipv6-access-list stats <IPv6-ACCESS-LIST-NAME> {(on <DEVICE-NAME>)}
```

#### Parameters

```
show ipv6-access-list stats <IPv6-ACCESS-LIST-NAME> {(on <DEVICE-NAME>)}
```

|                         |                                                                                                                                                                                                                                       |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ipv6-access-list stats  | Displays IPv6 access list related information and statistics                                                                                                                                                                          |
| <IPv6-ACCESS-LIST-NAME> | Optional. Displays statistics for a specified IPv6 access list. Specify the IPv6 access list name.<br>If IPv6 ACL name is not provided, the system displays statistics for all ACLs configured and applied.                           |
| on <DEVICE-NAME>        | Optional. Displays all or a specified IPv6 access list statistics on a specified device <ul style="list-style-type: none"><li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li></ul> |

#### Examples

```
nx9500-6C8809#show ipv6-access-list stats
IPv6 Access-list: test
 deny ipv6 any any rule-precedence 20 Hitcount: 4

nx9500-6C8809#
```

### l2tpv3

Displays a L2TPv3 (Layer 2 Tunnel Protocol Version 3) session information



#### Note

This command is not available in the USER EXEC mode.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000

- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show l2tpv3 {on/tunnel/tunnel-summary}
show l2tpv3 {on <DEVICE-NAME>}
show l2tpv3 {tunnel <L2TPv3-TUNNEL-NAME>} {session <L2TPv3-SESSION-NAME>} {on <DEVICE-NAME>}}
show l2tpv3 {tunnel-summary} {down/on/up}
show l2tpv3 {tunnel-summary} {on <DEVICE-NAME>}
show l2tpv3 {tunnel-summary} {down/up} {on <DEVICE-NAME>}
```

### Parameters

```
show l2tpv3 {on <DEVICE-NAME>}
```

|                           |                                                                                                                                                                                                                                                                                                          |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| l2tpv3 {on <DEVICE-NAME>} | <p>Displays L2TPv3 tunnel and session details or summary</p> <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; - Optional. Displays L2TPv3 information on a specified device</li> <li>• &lt;DEVICE-NAME&gt; - Specify the name of AP, wireless controller, or service platform.</li> </ul> |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
show l2tpv3 {tunnel <L2TPv3-TUNNEL-NAME>} {session <L2TPv3-SESSION-NAME>} {(on <DEVICE-NAME>)}
```

|                               |                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| l2tpv3                        | Displays L2TPv3 tunnel and session details or summary                                                                                                                                                                                                                                                                                                                                                       |
| tunnel <L2TPv3-TUNNEL-NAME>   | <p>Optional. Displays a specified L2TPv3 tunnel information</p> <ul style="list-style-type: none"> <li>• &lt;L2TPv3-TUNNEL-NAME&gt; - Specify the L2TPv3 tunnel name.</li> </ul>                                                                                                                                                                                                                            |
| session <L2TPv3-SESSION-NAME> | <p>Optional. Displays a specified L2TPv3 tunnel session information</p> <ul style="list-style-type: none"> <li>• &lt;L2TPv3-SESSION-NAME&gt; - Specify the session name.</li> </ul>                                                                                                                                                                                                                         |
| on <DEVICE-NAME>              | <p>The following keyword is recursive and common to the 'session &lt;L2TPv3-SESSION-NAME&gt;' parameter.</p> <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; - Optional. Displays a L2TPv3 tunnel and session details, based on the parameters passed, on a specified device.</li> <li>• &lt;DEVICE-NAME&gt; - Specify the name of AP, wireless controller, or service platform.</li> </ul> |

```
show l2tpv3 {tunnel-summary} {on <DEVICE-NAME>}
```

|                                   |                                                                                                                                                                                                                                                                                                |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| l2tpv3                            | <p>Displays L2TPv3 tunnel and session details or summary</p> <p><b>Note:</b> For an L2TPv3 tunnel over Auto IPsec, the tunnel status is displayed as: Established (secured by ipsec)</p>                                                                                                       |
| tunnel-summary {on <DEVICE-NAME>} | <p>Optional. Displays L2TPv3 tunnel summary</p> <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; - Optional. Displays L2TPv3 tunnel summary on a specified device</li> <li>• &lt;DEVICE-NAME&gt; - Specify the name of AP, wireless controller, or service platform.</li> </ul> |

```
show l2tpv3 {tunnel-summary} {down/up} {on <DEVICE-NAME>}
```

|                |                                                                          |
|----------------|--------------------------------------------------------------------------|
| l2tpv3         | Displays L2TPv3 tunnel and session details or summary                    |
| tunnel-summary | Optional. Displays L2TPv3 tunnel summary, based on the parameters passed |
| down           | Optional. Displays un-established tunnels summary                        |



|                  |                                                                                                                                                                                                                                                                                                                                                    |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| up               | Optional. Displays established tunnels summary                                                                                                                                                                                                                                                                                                     |
| on <DEVICE-NAME> | <p>The following keyword is common to the 'down' and 'up' parameters:</p> <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; - Optional. Displays summary, for un-established or established tunnels, on a specified device</li> <li>&lt;DEVICE-NAME&gt; - Specify the name of AP, wireless controller, or service platform.</li> </ul> |

## Examples

```
ap7161-11E6C4#show l2tpv3 tunnel-summary
```

```

Sl No Tunnel Name Tunnel State Estd/Total Sessions Encapsulation
Protocol
```

```

1 testTunnel Established (secured by ipsec) 1/1 IP
```

```
Total Number of Tunnels 1
```

```
ap7161-11E6C4#
```

```
ap7161-11E6C4#show l2tpv3
```

```

Tunnel Name : testTunnel
```

```
Control connection id : 2238970979
```

```
Peer Address : 30.1.1.1
```

```
Local Address : 30.1.1.30
```

```
Encapsulation Protocol : IP
```

```
MTU : 1460
```

```
Peer Host Name : rfss
```

```
Peer Vendor Name : Example Company
```

```
Peer Control Connection ID : 322606389
```

```
Tunnel State : Established (secured by ipsec)
```

```
Establishment Criteria : always
```

```
Sequence number of the next msg to the peer : 29
```

```
Expected sequence number of the next msg from the peer : 42
```

```
Sequence number of the next msg expected by the peer : 29
```

```
Retransmission count : 0
```

```
Reconnection count : 0
```

```
Uptime : 0 days 1 hours 2 minutes 47 seconds
```

```

Session Name : session1
```

```
VLANs : 30
```

```
Pseudo Wire Type : Ethernet_VLAN
```

```
Serial number for the session : 6
```

```
Local Session ID : 129538998
```

```
Remote Session ID : 8151374
```

```
Size of local cookie (0, 4 or 8 bytes) : 0
```

```
First word of local cookie : 0
```

```
Second word of local cookie : 0
```

```
Size of remote cookie (0, 4 or 8 bytes) : 0
```

```
First word of remote cookie : 0
```

```
Second word of remote cookie : 0
```

```
Session state : Established
```

```
Remote End ID : 444
```

```
Trunk Session : 1
```

```
Native VLAN tagged : Enabled
```

```
Native VLAN ID : 0
```

```
Number of packets received : 0
```

```
Number of bytes received : 0
```

```
Number of packets sent : 0
```

```
Number of bytes sent : 0
```

```
Number of packets dropped : 0
```

```
ap7161-11E6C4#
```

## lACP

Displays LACP (Link Aggregation Control Protocol) related information



### Note

For more information on enabling dynamic LACP, see [lACP](#) on page 1029 (profile - inf - ge - config mode), [lACP-channel-group](#) on page 1029 (profile - inf - ge - config mode), and [lACP](#) on page 1265 (device config mode).

### Supported in the following platforms:

- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show lACP [<1-4>|counters|details|sys-id]
show lACP <1-4> ([counters|details])
show lACP sys-id
```

### Parameters

```
show lACP <1-4> ([counters|details])
```

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show lACP <1-4> | Shows the LACP related information for a specified port-channel or all port-channels using LACP <ul style="list-style-type: none"><li>• &lt;1-4&gt; - Select the port-channel index number from 1 - 4. Note, LACP is supported only on the NX 5500, NX 7510, and NX 95XX model service platforms. However, the NX 95XX series service platforms support only two (2) port-channels. Where as the other model service platforms support four (4) port-channels.</li></ul> If the port-channel index number is not specified, the system displays LACP counters and details for all port-channels configured on the device. |
| counters        | Shows LACP counters for LACP-enabled port-channels. When passed without the <1-4> keyword, the system displays LACP counters for all configured port-channels. However, if the port-channel index number is specified, the system displays LACP counters only for the specified port-channel.                                                                                                                                                                                                                                                                                                                             |
| details         | Shows details for LACP-enabled port-channels. When passed without the <1-4> keyword, the system displays LACP details for all configured port-channels. However, if the port-channel index number is specified, the system displays LACP details only for the specified port-channel.                                                                                                                                                                                                                                                                                                                                     |

```
show lACP sys-id
```

|                  |                                                                                                                                                                                                                                              |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show lACP sys-id | Shows the LACP related information for all LACP-enabled port-channels <ul style="list-style-type: none"><li>• sys-id - Shows the LACP system identifier and priority. This is the identifier assigned to the LACP peers (devices).</li></ul> |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
NOC-controller#show interface port-channel 1
Interface port-channell is UP
 Hardware-type: aggregate, Mode: Layer 2, Address: 84-24-8D-7F-35-C8
 Index: 2018, Metric: 1, MTU: 1500
 Speed: Admin Auto, Operational 20G, Maximum 20G
 Duplex: Admin Auto, Operational Full
 Active-medium: n/a
 Channel-members: xge1 xge2
```

```

Switchport settings: trunk, access-vlan: n/a
 Input packets 5121052, bytes 807510883, dropped 0
 Received 5121052 unicasts, 0 broadcasts, 516544 multicasts
 Input errors 0, runts 0, giants 0
 CRC 0, frame 0, fragment 0, jabber 0
 Output packets 4804420, bytes 1053174746, dropped 0
 Sent 4804420 unicasts, 0 broadcasts, 0 multicasts
 Output errors 0, collisions 0, late collisions 0
 Excessive collisions 0

```

```

NOC-controller#
NOC-controller#show interface port-channel 4
Interface port-channel4 is UP
 Hardware-type: aggregate, Mode: Layer 2, Address: 84-24-8D-7F-35-C4
 Index: 2016, Metric: 1, MTU: 1500
 Speed: Admin Auto, Operational 4G, Maximum 4G
 Duplex: Admin Auto, Operational Full
 Active-medium: n/a
 Channel-members: ge2 ge3 ge4 ge5
 Switchport settings: trunk, access-vlan: n/a
 Input packets 5848499493, bytes 8772550780653, dropped 0
 Received 5848499493 unicasts, 0 broadcasts, 120167 multicasts
 Input errors 0, runts 0, giants 0
 CRC 0, frame 0, fragment 0, jabber 0
 Output packets 362245, bytes 33129264, dropped 0
 Sent 362245 unicasts, 0 broadcasts, 0 multicasts
 Output errors 0, collisions 0, late collisions 0
 Excessive collisions 0

```

```

NOC-controller#
NOC-controller#show lacp counters

```

| Port-Channel |      | Interface | LACPDU |       | Marker |      |
|--------------|------|-----------|--------|-------|--------|------|
| Packet error |      |           | Sent   | Recv  | Sent   | Recv |
| Sent         | Recv |           |        |       |        |      |
| pcl          |      | xge1      | 11548  | 12479 | 0      | 0    |
| 0            | 0    |           |        |       |        |      |
| pcl          |      | xge2      | 11550  | 12469 | 0      | 0    |
| 0            | 0    |           |        |       |        |      |
| pc4          |      | ge2       | 14081  | 14041 | 0      | 0    |
| 0            | 0    |           |        |       |        |      |
| pc4          |      | ge3       | 15877  | 15874 | 0      | 0    |
| 0            | 0    |           |        |       |        |      |
| pc4          |      | ge4       | 15875  | 15874 | 0      | 0    |
| 0            | 0    |           |        |       |        |      |
| pc4          |      | ge5       | 14064  | 14052 | 0      | 0    |
| 0            | 0    |           |        |       |        |      |

```

NOC-controller#

```

```

NOC-controller#show lacp details
Port-Channel pcl Interface xge1:
 Actor admin port key : 1
 Actor oper port key : 1
 Actor port priority : 32768
 Actor port number : 2011
 Actor admin port state : ActiveLACP LongTimeout Aggregatable OUT_OF_SYNC
Defaulted
 Actor oper port state : ActiveLACP LongTimeout Aggregatable IN_SYNC
Collecting Distributing
 Partner admin system ID : 32768, 00-00-00-00-00-00
 Partner oper system ID : 32768, 44-03-A7-BF-00-00
 Partner admin key : 0
 Partner oper key : 1
 Partner admin port priority : 0

```

```

Partner oper port priority : 32768
Partner admin port number : 0
Partner oper port number : 286
Partner admin port state : PassiveLACP LongTimeout Aggregatable OUT_OF_SYNC
Defaulted
Partner oper port state : ActiveLACP LongTimeout Aggregatable IN_SYNC
Collecting Distributing
Receive machine state : Current
Periodic transmission machine state : Slow periodic
Mux machine state : Collecting/Distributing
Port-Channel pcl Interface xge2:
Actor admin port key : 1
Actor oper port key : 1
Actor port priority : 32768
Actor port number : 2012
Actor admin port state : ActiveLACP LongTimeout Aggregatable OUT_OF_SYNC
Defaulted
--More--
NOC-controller#

```

### ldap-agent

Displays an LDAP agent's join status (join status to a LDAP server domain)

Use this command When LDAP is specified the external resource (as opposed to local RADIUS resources) to validate PEAP-MS-CHAP v2 authentication requests, user credentials, and password information needs to be made available locally to successfully connect to the external LDAP server. Up to two LDAP Agents (primary and secondary external resources) can be defined as external resources for PEAP-MS-CHAP v2 authentication requests.



#### Note

This command is not available in USER EXECUTABLE ,mode

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show ldap-agent join-status {on <DEVICE-NAME>}
```

### Parameters

|                  |                                                                                                                                                                                                                                                                                           |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ldap-agent       | Displays LDAP agent related configuration                                                                                                                                                                                                                                                 |
| join-status      | Displays if the LDAP agent has successfully joined a LDAP server's domain                                                                                                                                                                                                                 |
| on <DEVICE-NAME> | Optional. Displays if the LDAP agent has successfully joined a specified LDAP server's domain. <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the device running the LDAP server (access point, wireless controller, or service platform).</li> </ul> |

### Examples

```

nx9500-6C8809#show ldap-agent join-status
Primary LDAP Server's agent join-status : Joined domain TEST.

```

```
Secondary LDAP Server's agent join-status : Not Configured
nx9500-6C8809#
```

## licenses

Displays installed licenses and usage information

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show licenses {borrowed|lent}
```

### Parameters

```
show licenses {borrowed|lent}
```

|                          |                                                                                                                                                                                                                                      |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| licenses {borrowed lent} | Displays installed licenses and usage information <ul style="list-style-type: none"><li>• borrowed - Optional. Displays information on licenses borrowed</li><li>• lent - Optional. Displays information on licenses lent.</li></ul> |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Usage Guidelines

The WiNG HM network defines a three-tier structure, consisting of multiple wireless sites managed by a single NOC controller, The NOC and the site controllers constitute the first and second tiers of the hierarchy respectively. The site controllers in turn adopt and manage Access Points that form the third tier of the hierarchy. The site controllers may or may not be grouped to form clusters.

At the time of adoption, Access Points and adaptive Access Points are provided license by the adopting controller. These license packs can be installed on both the NOC and site controllers. When a AP/AAP is adopted by a controller, the controller pushes a license on to the device. At this point the various possible scenarios are:

- AP/AAP license packs installed on the NOC controller only. The NOC controller provides the site controllers with the AP licenses, ensuring that per platform limits are not exceeded.
- AP/AAP license packs installed on the NOC and site controllers. The site controller uses its installed licenses and, in case of a shortage, the site controller borrows additional licenses from the NOC. If the NoC controller is unable to allocate sufficient licenses, the site controller unadopts some of the AP/AAPs.
- AP/AAP license packs installed on one controller within a cluster. The site controller shares its installed and borrowed licenses with other cluster controllers.

### Examples

```
rfs4000-229D58#show licenses
Serial Number : 9184521800027
```

```
Device Licenses:
AP-LICENSE
String : DEFAULT-6AP-LICENSE
Value : 6
```

```

 Borrowed : 0
 Total : 6
 Used : 0
 AAP-LICENSE
 String :
 Value : 0
 Borrowed : 0
 Total : 0
 Used : 0
 ADVANCED-SECURITY
 String : DEFAULT-ADV-SEC-LICENSE
rfs4000-229D58#

```

The following example shows the **show > licenses** command output on a NOC controller:

```

NOC-NX9500#show licenses
Serial Number : B4C7996C8809

```

```

Device Licenses:
 AP-LICENSE
 String :
 Value : 0
 Lent : 0
 Total : 0
 Used : 0
 AAP-LICENSE
 String :
66069c24b3bb1259b34ff016c723a9e299dd408f0ff891e7c5f7e279a382648397d6b3e975e356a1
 Value : 10250
 Lent : 1
 Total : 10249
 Used : 2
 HOTSPOT-ANALYTICS
 String :
66069c24b3bb1259eb36826cab3cc83999dd408f0ff891e74b62b2d3594f0b3dde7967f30e49e497
 NSIGHT
 String :
66069c24b3bb12596b3d07672fdf5ccc99dd408f0ff891e719a98e92028e10e7a7461de1b5e70f32
 Value : 50

```

Total Licenses Including Licenses in Adopted Controllers:

```

 AP-LICENSE
 Value : 8
 Used : 1
 AAP-LICENSE
 Value : 10250
 Used : 3

```

```

NOC-NX9500#
NOC-NX9500#show licenses lent

```

```


 MAC HOST-NAME TYPE LENT BORROWER-MAC BORROWER-HOST-NAME
 VALIDITY

 B4-C7-99-6C-88-09 NOC-NX9500 AAP 1 00-15-70-38-06-49 RFS6K-SITE1-VLAN20
 current

NOC-NX9500#

```

*lldp*

Displays LLDP (Link Layer Discovery Protocol) related information

## Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
show lldp [neighbors|report]
show lldp neighbors {on <DEVICE-NAME>}
show lldp report {detail/on}
show lldp report {detail} {(on <DEVICE-OR-DOMAIN-NAME>)}
```

## Parameters

```
show lldp neighbors {on <DEVICE-NAME>}
```

|                  |                                                                                                                                                                                                               |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| lldp             | Displays L2TPv3 neighbors table or aggregated LLDP neighbors table                                                                                                                                            |
| neighbors        | Displays LLDP neighbors table                                                                                                                                                                                 |
| on <DEVICE-NAME> | Optional. Displays L2TPv3 neighbors table on a specified device <ul style="list-style-type: none"><li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li></ul> |

```
show lldp report {detail} {(on <DEVICE-OR-DOMAIN-NAME>)}
```

|                            |                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| lldp                       | Displays L2TPv3 neighbors table or aggregated LLDP neighbors table                                                                                                                                                                                                                                                                                                          |
| report detail              | Displays aggregated LLDP neighbors table <ul style="list-style-type: none"><li>• detail - Optional. Displays detailed aggregated LLDP neighbors table</li></ul> <p><b>Note:</b> If the 'on' keyword is used without the 'detail' keyword, the system displays LLDP neighbors table summary on the specified device or RF Domain.</p>                                        |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is recursive and common to the 'report detail' parameter: <ul style="list-style-type: none"><li>• on &lt;DEVICE-OR-DOMAIN-NAME&gt; - Displays aggregated LLDP neighbors table on a specified device or RF Domain</li><li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; - Specify the name of the AP, wireless controller, service platform, or RF Domain.</li></ul> |

## Examples

```
nx9500-6C8809#show lldp neighbors

Chassis ID: 00-18-71-D0-0B-00
System Name: TechPubs-ProCurve-Switch
Platform: ProCurve J8697A Switch 5406z1, revision K.12.1X, ROM K.11.03 (/sw/code/build/
btm(sw_espl))
Capabilities: Bridge Router
Enabled Capabilities: Bridge
Local Interface: gel, Port ID(Port Description) (outgoing port): 5(A5)
TTL: 113 sec
Management Addresses: 192.168.13.40
nx9500-6C8809#
```

### logging

Displays the network's activity log

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show logging {on <DEVICE-NAME>}
```

### Parameters

```
show logging {on <DEVICE-NAME>}
```

|                            |                                                                                                                                                                                         |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| logging {on <DEVICE-NAME>} | Displays logging information on a specified device <ul style="list-style-type: none"><li>• &lt;DEVICE-NAME&gt; - Optional. Specify the name of the AP or wireless controller.</li></ul> |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
NOC-NX9500#show logging
```

```
Logging module: enabled
 Aggregation time: disabled
 Console logging: level debugging
 Monitor logging: disabled
 Buffered logging: level warnings
 Syslog logging: level warnings
 Facility: local7
```

```
Log Buffer (2096166 bytes):
```

```
Feb 09 10:49:16 2018: NOC-NX9500 : %DIAG-4-PWRSPLY_FAIL: Power supply redundancy failure
Feb 09 10:39:11 2018: NOC-NX9500 : %DIAG-4-PWRSPLY_FAIL: Power supply redundancy failure
Feb 09 10:29:06 2018: NOC-NX9500 : %DIAG-4-PWRSPLY_FAIL: Power supply redundancy failure
Feb 09 10:19:01 2018: NOC-NX9500 : %DIAG-4-PWRSPLY_FAIL: Power supply redundancy failure
Feb 09 10:08:55 2018: NOC-NX9500 : %DIAG-4-PWRSPLY_FAIL: Power supply redundancy failure
Feb 09 09:58:49 2018: NOC-NX9500 : %DIAG-4-PWRSPLY_FAIL: Power supply redundancy--More--
NOC-NX9500#
```

### *mac-access-list-stats*

Displays MAC access list related statistics



#### Note

This command is not present in USER EXEC mode.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show mac-access-list-stats {<MAC-ACCESS-LIST-NAME>/on}
show mac-access-list-stats {<MAC-ACCESS-LIST-NAME>} {(on <DEVICE-NAME>)}
```



## Parameters

```
show mac-access-list-stats {<MAC-ACCESS-LIST-NAME>} {(on <DEVICE-NAME>)}
```

|                       |                                                                                                                                                                                                                                    |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mac-access-list-stats | Displays MAC access list statistics                                                                                                                                                                                                |
| <MAC-ACCESS-LIST>     | Optional. Displays statistics for a specified MAC access list. Specify the MAC access list name.<br><br><b>Note:</b> The system displays all configured ACL statistics if no ACL name is specified.                                |
| on <DEVICE-NAME>      | Optional. Displays all or a specified MAC access list statistics on a specified device <ul style="list-style-type: none"><li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li></ul> |

## Examples

```
nx9500-6C8809#show mac-access-list stats scalemacacl | i 311
 permit D0-67-E5-3F-C0-00 FF-FF-FF-FF-F0-00 host 00-1E-EC-F2-0A-76 rule-precedence 311
Hitcount: 0 Hardware Hitcount: 0
nx9500-6C8809#
```

## mac-address-table

Displays MAC address table entries

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
show mac-address-table {on <DEVICE-NAME>}
```

## Parameters

```
show mac-address-table {on <DEVICE-NAME>}
```

|                   |                                                                                                                                                                                                                |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mac-address-table | Displays MAC address table entries                                                                                                                                                                             |
| on <DEVICE-NAME>  | Optional. Displays MAC address table entries on a specified device <ul style="list-style-type: none"><li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li></ul> |

## Examples

```
NOC-NX9500#show mac-address-table
```

```

```

| BRIDGE | VLAN | PORT | MAC               | STATE   |
|--------|------|------|-------------------|---------|
| 1      | 172  | ge2  | 5C-0E-8B-1C-53-2C | forward |
| 1      | 1    | ge1  | 00-18-71-D0-1B-E6 | forward |
| 1      | 172  | ge2  | 5C-0E-8B-1C-53-2D | forward |
| 1      | 1    | ge1  | 74-67-F7-07-02-35 | forward |
| 1      | 1    | ge1  | 84-24-8D-84-A2-24 | forward |
| 1      | 1    | ge1  | 00-04-96-9C-F1-25 | forward |
| 1      | 1    | ge1  | 84-24-8D-DF-9A-4C | forward |
| 1      | 1    | ge1  | B4-C7-99-71-17-28 | forward |

```

```

```
Total number of MACs displayed: 8
NOC-NX9500#
```

## macauth

Displays details of wired ports that have MAC address authentication enabled.

Use this command to view MAC authentication configuration and authentication state. The command displays the current authentication state of the wired host, the authorization state of the Ge1 port, and the wired hosts' MAC address. The port status displays as Authorized if the wired host has successfully authenticated and Not Authorized if the wired host has not authenticated or has failed MAC authentication.

For more information on enabling MAC address authentication on a wired port, see [mac-auth](#) on page 1183 (profile-config-mode).

### Supported in the following platforms:

- Wireless Controllers — RFS 4000

### Syntax

```
show mac-auth {all|interface|on}
show mac-auth {all|interface [<INTERFACE-NAME>|ge <1-5>|port-channel <1-3>|
t1e1 <1-4>|up <1-2>|xge <1-4>]} {(on <DEVICE-NAME>)}
```

### Parameters

```
show mac-auth {all|interface [<INTERFACE-NAME>|ge <1-5>|port-channel <1-3>|
t1e1 <1-4>|up <1-2>|xge <1-4>]} {(on <DEVICE-NAME>)}
```

|                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| macauth                                                                                | Displays MAC authentication related information for all interfaces or a specified interface                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| all                                                                                    | <ul style="list-style-type: none"> <li>• Displays MAC authentication related information for all interfaces</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| interface [<INTERFACE-NAME> ge <1-5> port-channel <1-3> t1e1 <1-4> up <1-2> xge <1-4>] | <p>Optional. Displays MAC authentication related information for a specified interface. Specify the interface using one of the following options:</p> <ul style="list-style-type: none"> <li>• &lt;INTERFACE-NAME&gt; - Selects the interface identified by the &lt;INTERFACE-NAME&gt; keyword</li> <li>• ge &lt;1-5&gt; - Selects the GigabitEthernet interface identified by the index number</li> <li>• port-channel &lt;1-3&gt; - Selects the port channel interface identified by the index number</li> <li>• t1e1 &lt;1-4&gt; - Selects the layer 2 interface (Ethernet port)</li> <li>• up &lt;1-2&gt; - Selects the WAN Ethernet interface identified by the index number</li> <li>• xge &lt;1-4&gt; - Selects the TenGigabitEthernet interface identified by the index number</li> </ul> |
| on <DEVICE-NAME>                                                                       | <p>The following keywords are common to the 'all' and 'interface' parameters:</p> <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; - Optional. Displays MAC authentication related information on a specified device</li> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> <p><b>Note:</b> When the 'on' keyword is used exclusively, without the 'all' and 'interface' options, the system displays MAC authentication related information for interfaces configured on the specified device.</p>                                                                                                                                                                                                                     |

## Examples

```
rfs4000-229D58(config)#show mac-auth all
AAA-Policy is none
```

```
Mac Auth info for interface GE1

Mac Auth Enabled
Mac Auth Not Authorized

Mac Auth info for interface GE2

Mac Auth Disabled
Mac Auth Not Authorized

Mac Auth info for interface GE3

Mac Auth Disabled
Mac Auth Not Authorized

Mac Auth info for interface GE4

Mac Auth Disabled
Mac Auth Authorized

Mac Auth info for interface GE5

Mac Auth Disabled
Mac Auth Not Authorized

Mac Auth info for interface UP1

Mac Auth Disabled
Mac Auth Not Authorized
rfs4000-229D58(config)#
```

### *mac-auth-clients*

Displays MAC authenticated clients

#### **Supported in the following platforms:**

- Wireless Controllers — RFS 4000

#### **Syntax**

```
show mac-auth-clients [all|interface]
show mac-auth-clients all {on <DEVICE-NAME>}
show mac-auth-clients interface {<INF-NAME>|ge <1-X>|port-channel <1-2>|xge <1-4>}
```

#### **Parameters**

```
show mac-auth-clients all {on <DEVICE-NAME>}
```

|                  |                                                                                                                                                                                                                                       |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mac-auth-clients | Displays MAC authenticated clients based on the parameters passed. The options are: all and interface.                                                                                                                                |
| all              | Displays MAC authenticated clients for all interfaces                                                                                                                                                                                 |
| on <DEVICE-NAME> | Optional. Displays MAC authenticated clients for all interfaces on a specified device <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
show mac-auth-clients interface {<INF-NAME>/ge <1-X>/port-channel <1-2>/xge <1-4>}
```

|                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mac-auth-clients                                                | Displays MAC authenticated clients based on the parameters passed. The options are: all and interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| interface [<INF-NAME>] ge <1-X>  port-channel <1-2>  xge <1-4>] | Displays MAC authenticated clients for the specified interface. Select the interface type from the following options: <ul style="list-style-type: none"> <li>• &lt;INF-NAME&gt; – Optional. Displays MAC authenticated clients for the interface identified by the &lt;INF-NAME&gt; keyword. Specify the layer 2 (ethernet port) interface name.</li> <li>• ge &lt;1-X&gt; – Optional. Displays MAC authenticated clients for the selected GigabitEthernet interface. Specify the GE interface index from 1 - X. This will vary for different device types.</li> <li>• port-channel &lt;1-2&gt; – Optional. Displays MAC authenticated clients for the selected port channel interface. Specify the port channel interface index from 1 - 2.</li> <li>• xge &lt;1-4&gt; – Optional. Displays MAC authenticated clients for the selected TenGigabitEthernet interface. Specify the interface index from 1 - 4.</li> </ul> |
| on <DEVICE-NAME>                                                | Optional. Displays MAC authenticated clients for the specified interface on a specified device <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

### Examples

```
rfs4000-229D58(config-device-B4-C7-99-22-9D-58)#show mac-auth-clients interface ge 1

MAC STATE INTERFACE

Total number of MACs displayed: 0
rfs4000-229D58(config-device-B4-C7-99-22-9D-58)#
```

### mint

Displays MiNT protocol related statistics and configuration

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
show mint [config|dis|id|info|known-adopters|links|lsp|lsp-db|mlcp|neighbors|route|
 stats|tunnel-controller|tunneled-vlans]
show mint [config|id|info|known-adopters|route|stats|tunneled-vlans] {on <DEVICE-NAME>}
show mint [dis|links|neighbors|tunnel-controller] {details} {(on <DEVICE-NAME>)}
show mint lsp
show mint lsp-db {details <MINT-ADDRESS>} {(on <DEVICE-NAME>)}
show mint mlcp {history} {(on <DEVICE-NAME>)}
```

## Parameters

```
show mint [config|id|info|known-adopters|route|stats|tunneled-vlans]
{on <DEVICE-NAME>}
```

|                  |                                                                                                                                                                                                                                                                                                               |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mint             | Displays MiNT protocol information based on the parameters passed                                                                                                                                                                                                                                             |
| config           | Displays MiNT configuration                                                                                                                                                                                                                                                                                   |
| id               | Displays local MiNT ID                                                                                                                                                                                                                                                                                        |
| info             | Displays MiNT status                                                                                                                                                                                                                                                                                          |
| known-adopters   | Displays known, possible, or reachable adopters                                                                                                                                                                                                                                                               |
| route            | Displays MiNT route table details                                                                                                                                                                                                                                                                             |
| stats            | Displays MiNT related statistics                                                                                                                                                                                                                                                                              |
| tunneled-vlans   | Displays MiNT tunneled VLAN details                                                                                                                                                                                                                                                                           |
| on <DEVICE-NAME> | The following keywords are common to all of the above parameters: <ul style="list-style-type: none"><li>on &lt;DEVICE-NAME&gt; - Optional. Displays MiNT protocol details on a specified device</li><li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li></ul> |

```
show mint [dis|links|neighbors|tunnel-controller] {details} {(on <DEVICE-NAME>)}x
```

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mint                          | Displays MiNT protocol information based on the parameters passed                                                                                                                                                                                                                                                                                                                                                                                                                           |
| dis                           | Displays MiNT network DISes (Designated Intermediate Systems) and EVISes (Ethernet Virtualization Interconnects)                                                                                                                                                                                                                                                                                                                                                                            |
| links                         | Displays MiNT networking link details                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| neighbors                     | Displays adjacent MiNT peer details                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| tunnel-controller             | Displays details of MiNT VLAN network tunnel wireless controllers for extended VLAN load balancing                                                                                                                                                                                                                                                                                                                                                                                          |
| details {(on <DEVICE-NAME>)}x | The following keywords are common to the 'dis', 'links', 'neighbors', and 'tunnel-controller' parameters: <ul style="list-style-type: none"><li>details - Optional. Displays detailed MiNT information</li><li>on &lt;DEVICE-NAME&gt; - Optional. This is a recursive parameter, which displays MiNT information on a specified device<ul style="list-style-type: none"><li>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li></ul></li></ul> |

```
show mint lsp
```

|      |                                                                   |
|------|-------------------------------------------------------------------|
| mint | Displays MiNT protocol information based on the parameters passed |
| lsp  | Displays this router's MiNT LSPs (Label Switched Paths)           |

```
show mint lsp-db {details <MINT-ADDRESS>} {(on <DEVICE-NAME>)}
```

|                        |                                                                                                                                                                                                                                                                                                                                  |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mint                   | Displays MiNT protocol information based on the parameters passed                                                                                                                                                                                                                                                                |
| lsp-db                 | Displays MiNT LSP database entries                                                                                                                                                                                                                                                                                               |
| details <MINT_ADDRESS> | Optional. Displays detailed MiNT LSP database entries <ul style="list-style-type: none"> <li>• &lt;MINT_ADDRESS&gt; - Specify the MiNT address in the AA.BB.CC.DD format.</li> </ul>                                                                                                                                             |
| on <DEVICE-NAME>       | The following keyword is recursive and common to the 'details' parameter: <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; - Optional. Displays MiNT LSP database entries on a specified device</li> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
show mint mlcp {history} {(on <DEVICE-NAME>)}
```

|                  |                                                                                                                                                                                                                                                                                                                            |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mint             | Displays MiNT protocol information based on the parameters passed<br>This command displays the 'hello-interval' and 'hold-time' default values for both IP and VLAN links.                                                                                                                                                 |
| mlcp             | Displays MLCP (MiNT Link Creation Protocol ) status                                                                                                                                                                                                                                                                        |
| history          | Optional. Displays MLCP client history                                                                                                                                                                                                                                                                                     |
| on <DEVICE-NAME> | The following keyword is recursive and common to the 'history' parameter: <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; - Optional. Displays MLCP client history on a specified device</li> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

## Examples

```
NOC-NX9500#show mint stats
2 Level-1 neighbors
Level-1 LSP DB size 5 LSPs (1 KB)
Last Level-1 SPF took 0.000s
Level-1 SPF (re)calculated 6 times.
5 Level-1 paths.
0 Level-2 neighbors
Level-2 LSP DB size 0 LSPs (0 KB)
Last Level-2 SPF took 0.000s
Level-2 SPF (re)calculated 0 times.
0 Level-2 paths.
NOC-NX9500#
NOC-NX9500#show mint lsp
id 19.6C.88.09, level 1, 2 adjacencies, 0 extended-vlans
seqnum 1519955, expires in 22 minutes, republish in 774 seconds
90 bytes, can-adopt: True, adopted-by: 00.00.00.00, dis-priority 5, Level-2-gateway: False
hostname "NOC-NX9500"
rf-domain "default", priority vector: 0xe0dc0000
adjacent to 70.38.06.49, cost 100
```

```

adjacent to 19.6D.B5.D4, cost 100
NOC-NX9500#
NOC-NX9500#show mint lsp-db
5 LSPs in LSP-db of 19.6C.88.09:
LSP 19.6C.88.09 at level 1, hostname "NOC-NX9500", 2 adjacencies, seqnum 1519955
LSP 19.6D.B5.D4 at level 1, hostname "RFS6K-SITE2-VLAN192", 2 adjacencies, seqnum 1972642
LSP 19.74.B4.5C at level 1, hostname "ap8132-74B45C", 1 adjacencies, seqnum 1742227
LSP 4D.83.30.A4 at level 1, hostname "ap7522-8330A4", 1 adjacencies, seqnum 519924
LSP 70.38.06.49 at level 1, hostname "RFS6K-SITE1-VLAN20", 2 adjacencies, seqnum 1391030
NOC-NX9500#
NOC-NX9500#show mint route
Destination : Next-Hop(s)
19.6D.B5.D4 : 19.6D.B5.D4 via ip-192.168.13.2:24576
19.74.B4.5C : 19.6D.B5.D4 via ip-192.168.13.2:24576
19.6C.88.09 : 19.6C.88.09 via self
70.38.06.49 : 70.38.06.49 via ip-20.168.10.2:24576
4D.83.30.A4 : 70.38.06.49 via ip-20.168.10.2:24576
NOC-NX9500#
NOC-NX9500#show mint config
Base priority 5
DIS priority 5
Control priority 220
UDP/IP Mint encapsulation port 24576
Global Mint MTU 1500
NOC-NX9500#
NOC-NX9500#show mint mlcp
MLCP VLAN state: MLCP_INIT
MLCP VLAN Hello Interval: 4s(default), Adjacency hold time: 13s(default)
 Potential VLAN links: None
 All VLANs were scanned 1 times
MLCP IP: ENABLED
MLCP IPv6: ENABLED
MLCP IP/IPv6 state: MLCP_INIT
MLCP IP Hello Interval: 15s(default), Adjacency hold time: 46s(default)
 Potential L3 Links:
 None
NOC-NX9500#

```

## *nsight*

Displays NSight related information and also displays the database server status (reachable or not)

### **Supported in the following platforms:**

- Service Platforms — NX 95XX, NX 96XX, VX 9000

### **Syntax**

```
show nsight status
```

### **Parameters**

```
show nsight status
```

|               |                                                                                                                                                                                                                                                                                                                                                                          |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| nsight status | <p>Displays the NSight module related status, such as</p> <ul style="list-style-type: none"> <li>• NSight is enabled or not on the device</li> <li>• NSight report and aggregation daemon is running or not</li> <li>• NSight alarm daemon is running or not</li> <li>• NSight server daemon is running or not</li> <li>• Database server is reachable or not</li> </ul> |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config)#show nsight status
Naight is enabled
 Naight report and aggregation daemon is running
 Naight alarm daemon is running
 Naight server daemon is running
 Database server is local
 Database server is reachable
nx9500-6C8809(config)#
```

## ntp

Displays NTP (Network Time Protocol) information. NTP enables clock synchronization within a network.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show ntp [associations|status]
show ntp [associations {detail/on}|status {on <DEVICE-NAME>}]
```

### Parameters

```
show ntp [associations {detail/on}|status {on <DEVICE-NAME>}]
```

|                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>ntp associations {detail/on}</code>        | <p>Displays existing NTP associations. The interaction between the controller or service platform and a SNTP server constitutes an association. SNTP associations are of two kinds:</p> <ul style="list-style-type: none"><li>• peer associations - where a controller or service platform synchronizes to another system or allows another system to synchronize to it, or</li><li>• - server associations - where only the controller or service platform synchronizes to the SNTP resource, not the other way around.</li></ul> <p>Specify the following parameters to view NTP association details:</p> <ul style="list-style-type: none"><li>• detail - Optional. Displays detailed NTP associations<ul style="list-style-type: none"><li>• on &lt;DEVICE-NAME&gt; - Optional. Displays NTP associations on a specified device</li></ul></li></ul> <p>&lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</p> <p><b>Note:</b> If the 'on' keyword is used without the 'detail' keyword, the system displays a summary of existing NTP associations on the specified device or RF Domain.</p> |
| <code>ntp status {on &lt;DEVICE-NAME&gt;}</code> | <p>Displays the performance (status) information relative to the NTP association status. Use this command to view the access point, controller, or service platform's current NTP resource.</p> <ul style="list-style-type: none"><li>• on &lt;DEVICE-NAME&gt; - Optional. Displays NTP association status on a specified device</li><li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Examples

```
nx9500-6C8809#show ntp associations
```

---



```

STATUS NTP SERVER IP ADDR REF CLOCK IP ADDR STRATUM WHEN POLL REACH
DELAY OFFSET DISPERSION

~ 12.12.12.12 INIT 16 - 1024 0
0.0 0.0 15937.5
~ 11.11.11.11 INIT 16 - 1024 0
0.0 0.0 15937.5

```

```

STATUS Notation: * master (syncd), # master (unsyncd), + selected, - candidate, ~
configured
nx9500-6C8809#
nx9500-6C8809#show ntp status

```

| ITEM            | VALUE                                        |
|-----------------|----------------------------------------------|
| Leap            | Clock is unsynchronized                      |
| Stratum         | 16                                           |
| Reference       | INIT                                         |
| Frequency       | 0.0000 Hz                                    |
| Precision       | 2^-20                                        |
| Reference time  | 00000000.00000000 (Feb 07 11:58:16 UTC 2036) |
| Clock Offset    | 0.000 msec                                   |
| Root delay      | 0.000 msec                                   |
| Root Dispersion | 0.000 msec                                   |

```

nx9500-6C8809#

```

### *password-encryption*

Displays password encryption status (enabled/disabled)

#### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### **Syntax**

```
show password-encryption status
```

#### **Parameters**

```
show password-encryption status
```

|                            |                                                        |
|----------------------------|--------------------------------------------------------|
| password-encryption status | Displays password encryption status (enabled/disabled) |
|----------------------------|--------------------------------------------------------|

#### **Examples**

```

nx9500-6C8809(config)#show password-encryption status
Password encryption is enabled
nx9500-6C8809(config)#

```

### *pppoe-client*

Displays PPPoE client information

Use this command to view PPPoE statistics derived from access to high-speed data and broadband networks. PPPoE uses standard encryption, authentication, and compression methods as specified by the PPPoE protocol. PPPoE enables point-to-points connection to an ISP over existing Ethernet interface.

**Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

**Syntax**

```
show pppoe-client [configuration|status] {on <DEVICE-NAME>}
```

**Parameters**

```
show pppoe-client [configuration|status] {on <DEVICE-NAME>}
```

|                  |                                                                                                                                                                                                                                                                                                                                                          |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| pppoe-client     | Displays PPPoE client information (configuration and status)                                                                                                                                                                                                                                                                                             |
| configuration    | Displays detailed PPPoE client configuration                                                                                                                                                                                                                                                                                                             |
| status           | Displays detailed PPPoE client status                                                                                                                                                                                                                                                                                                                    |
| on <DEVICE-NAME> | The following keywords are common to 'configuration' and 'status' parameters: <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; - Optional. Displays detailed PPPoE client status or configuration on a specified device</li> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

**Examples**

```
nx9500-6C8809#show pppoe-client configuration
 PPPoE Client Configuration:
+-----+
| Mode : Disabled
| Service Name :
| Auth Type : pap
| Username :
| Password : fJx50+5duPjaOaPuXmtLDQAAAAAmvgEXcQ1+eUK4ByHK4aRi
| Idle Time : 600
| Keepalive : Disabled
| Local n/w : vlan1
| Static IP : __wing_internal_not_set__
| MTU : 1492
+-----+

nx9500-6C8809#
```

*privilege*

Displays the logged-in user's privilege level

**Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533

- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show privilege
```

### Parameters

None

### Examples

```
nx9500-6C8809(config)#show privilege
Current user privilege: superuser
nx9500-6C8809(config)#
```

## *radius*

Displays the amount of access time consumed and the amount of access time remaining for all guest users configured on a RADIUS server

Every captive portal guest user can access the captive portal for a specified duration. This results in following three scenarios:

- Scenario 1: Access duration not specified (in this case the default of 1440 minutes is applied)
- Scenario 2: Access duration is specified and is greater than 0
- Scenario 3: Access duration is specified and equals to 0 (in this case the guest user has unlimited access)

In all the three scenarios the access time consumed is the duration for which the guest user has logged.

But the access time remaining varies. It is calculated as follows:

- Scenarios 1 & 2 - It is the lesser of the following two values: difference between the configured access duration and the time consumed AND the time until user account expiration.
- Scenario 3 - It is the time until user account expiration.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show radius [guest-users|server]
show radius guest-users {brief|<GUEST-USER-NAME>}
show radius server
```

### Parameters

```
show radius guest-users {brief|<GUEST-USER-NAME>}
```

radius guest-users {brief|<GUEST-USER-NAME>}

Displays RADIUS server's guest user's access details: total time for which the user has logged in, and the amount of access time remaining.

- brief – Displays the total number of guest users provided RADIUS access
- <GUEST-USER-NAME> – Optional. Provide the name of the guest user (whose access details are to be viewed). If no name is provided, the system displays details of all guest users who have successfully logged in at least once.

Use this command in the captive-portal context to view time and data statistics for guest user(s) having bandwidth-based or time-based vouchers configured. In such a scenario, the system displays the following information: data configured, data remaining, and current bandwidths (for both downlink and uplink), time configured, and time remaining.

If bandwidth-based voucher is not applicable to a guest user, the data configured and data remaining values are displayed as 'unlimited'. The bandwidth columns are blank. If time-based voucher is not applicable to a guest user, the only value displayed is the time remaining (which is the time till the expiration of the guest user's account).

**Note:** For more information on configuring bandwidth-based and time-based vouchers, see [user](#) (radius user policy config mode).

show radius server

radius server

Displays RADIUS server related statistical data

## Examples

```
rfs4000-229D58#show radius guest-users
```

```
 TIME (min:sec)
USED REMAINING GUEST USER
0:00 9:00 time9
0:00 5:00 time5
0:00 15:00 time15
0:00 305416:35 notime
2:31 7:29 time10
```

```
rfs4000-229D58#
```

The following example shows a RADIUS user pool with guest users having bandwidth-based, time-based, bandwidth and time based, and no bandwidth or time based vouchers:

```
rfs4000-229D58(config-captive-portal-wdws)#show context
radius-user-pool-policy wdws
 user time_and_data password 0 both group wdws guest expiry-time 12:00 expiry-date
12/31/2015 access-duration 8000 data-limit 500 committed-downlink 3000 committed-
uplink 2000 reduced-downlink 1000 reduce4
 user neither password 0 nine group wdws guest expiry-time 12:00 expiry-date 12/31/2015
 user data_only password 0 data group wdws guest expiry-time 12:00 expiry-date 12/31/2015
data-limit 125 committed-downlink 1000 committed-uplink 800 reduced-downlink 500
reduced-uplink 400
rfs4000-229D58(config-captive-portal-wdws)#
```

The following example shows the captive portal access details for the above mentioned RADIUS user pool users:

```
rfs4000-229D58(config-captive-portal-wdws)#show radius guest-users
 TIME (DD:HH:MM:SS) DATA (kilobytes)
BANDWIDTH (kbps)
GUEST USER CONFIGURED REMAINING CONFIGURED REMAINING CFGD DN CURR
DN CFGD UP CURR UP
```

```

time_and_data 5:13:20:00 5:12:00:50 512000 433727 3000
0 2000 0
neither till expiry 221:19:44:54 unlimited unlimited
data_only till expiry 221:19:44:54 128000 127587 1000
0 800 0
time_only 3:11:20:00 3:11:19:47 unlimited unlimited
Current time: 17:15:07
rfs4000-229D58(config-captive-portal-wdws)#

```

## reload

Displays scheduled reload information for a specific device



### Note

This command is not present in the USER EXEC mode.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show reload {on <DEVICE-OR-DOMAIN-NAME>}
```

### Parameters

```
show reload {on <DEVICE-OR-DOMAIN-NAME>}
```

|                                     |                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| reload {on <DEVICE-OR-DOMAIN-NAME>} | <p>Displays scheduled reload information for a specified device</p> <ul style="list-style-type: none"> <li>• on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Displays configuration on a specified device</li> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```

nx9500-6C8809(config)#show reload
No reload is scheduled.
nx9500-6C8809(config)#

```

## rf-domain-manager

Displays RF Domain manager selection details

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show rf-domain-manager {on <DEVICE-OR-DOMAIN-NAME>}
```

## Parameters

```
show rf-domain-manager {on <DEVICE-OR-DOMAIN-NAME>}
```

|                            |                                                                                                                                                                                                                                                         |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| rf-domain-manager          | Displays RF Domain manager selection details                                                                                                                                                                                                            |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Displays RF Domain manager selection details on a specified device or domain <ul style="list-style-type: none"><li>&lt;DEVICE-OR-DOMAIN-NAME&gt; – specify the name of the AP, wireless controller, service platform, or RF Domain.</li></ul> |

## Examples

```
nx9500-6C8809#show rf-domain-manager
RF Domain TechPubs
RF Domain Manager:
 ID: 19.6C.88.09
Controller Managed
Device under query:
 Priority: 220
 Has IP MiNT links
 Has wired MiNT links
nx9500-6C8809#
```

## role

Displays role based firewall information

## Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
show role [ldap-stats|wireless-clients]
show role [ldap-stats|wireless-clients] {on <DEVICE-NAME>}
```

## Parameters

```
show role [ldap-stats|wireless-clients] {on <DEVICE-NAME>}
```

|                       |                                                                                                                                                                                                                                                                                                                                               |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| role ldap-stats       | Displays LDAP server status and statistics                                                                                                                                                                                                                                                                                                    |
| role wireless-clients | Displays clients associated with roles                                                                                                                                                                                                                                                                                                        |
| on <DEVICE-NAME>      | The following parameters are common to the 'ldap-stats' and 'wireless-clients' keywords: <ul style="list-style-type: none"><li>on &lt;DEVICE-NAME&gt; – Optional. Displays clients associated with roles on a specified device</li><li>&lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, and service platform.</li></ul> |

## Examples

```
nx9500-6C8809(config)#show role wireless-clients
No ROLE statistics found.
nx9500-6C8809(config)#
```

## route-maps

Displays route map statistics for defined routes

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show route-maps {on <DEVICE-NAME>}
```

### Parameters

```
show route-maps {on <DEVICE-NAME>}
```

|                  |                                                                                                                                                                                                             |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| route-maps       | Displays configured route map statistics for all defined routes<br>For more information on route maps, see <a href="#">route-map</a> .                                                                      |
| on <DEVICE-NAME> | Optional. Displays route map statistics on a specified device <ul style="list-style-type: none"><li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li></ul> |

### Examples

```
nx9500-6C8809(config)#show route-maps
nx9500-6C8809(config)#
```

## rtls

Displays RTLS (Real Time Location Service) statistics for Access Points contributing locationing information

### Supported in the following platforms:

- Access Points — AP 6522, AP 6532, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 81XX, AP 8232
- Wireless Controllers — RFS 4000, RFS 6000
- Service Platforms — NX 7500, NX 9500, NX 9510

### Syntax

```
show rtls [aer scout|ekahau|omnitrail] {<MAC/HOSTNAME>} {(on <DEVICE-OR-DOMAIN-NAME>)}
```

### Parameters

```
show rtls [aer scout|ekahau|omnitrail] {<MAC/HOSTNAME>} {(on <DEVICE-OR-DOMAIN-NAME>)}
```

|           |                                            |
|-----------|--------------------------------------------|
| rtls      | Displays Access Point RTLS statistics      |
| aer scout | Displays Access Point Aer scout statistics |
| ekahau    | Displays Access Point Ekahau statistics    |
| omnitrail | Displays access point Omnitrail statistics |

|                            |                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <MAC/HOSTNAME>             | Optional. Displays Aeroscout or Ekahau statistics for a specified Access Point. Specify the MAC address or hostname of the Access Point.                                                                                                                                                                                                                                            |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is recursive and common to all of the above parameters: <ul style="list-style-type: none"> <li>• on &lt;DEVICE-OR-DOMAIN-NAME&gt; - Optional. Displays Aeroscout or Ekahau statistics on a specified device or domain.</li> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; - Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> |

## Examples

```
rfs4000-229D58(config)#show rtls aeroscout
```

```
Aeroscout Engine IP: 0.0.0.0 Port: 0
Send Count : 0
Recv Count : 0
Tag Reports : 0
Nacks : 0
Acks : 0
Lbs : 0
AP Status : 0
AP Notif : 0
Send Err : 0
Errmsg Count : 0
```

```
Total number of APs displayed: 1
```

```
rfs4000-229D58(config)#
ap8533-84A224##show rtls omnitrail
Engine IP: 157.235.90.41
Control Port: 8890
Otls 2.4 GHz Engine status: CONNECTED
Otls 5 GHz Engine status: CONNECTED
Data Port configured for forwarding 2.4GHz Radio detected beacons: 8888
Data Port configured for forwarding 5GHz Radio detected beacons:8889
Heart beats sent for 2.4GHz Port : 1
Heart beats sent for 5GHz Port : 0
Beacon tags received on 2.4GHz Radio and forwarded: 6883
Beacon tags received on 5GHz Radio and forwarded: 0
Beacon tags received on Sensor Radio (2.4GHz Band) and forwarded: 5187
Beacon tags received on Sensor Radio (5Ghz Band) and forwarded: 0
Total number of APs displayed: 1
ap8533-84A224#
```

## *running-config*

Displays configuration files (where all configured MAC and IP access lists are applied to an interface)

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show running-config {aaa-policy/application/application-group/application-policy/
association-acl-policy/auto-provisioning-policy/captive-portal-policy/device/database-
client-policy/
database-policy/device/device-overrides/dhcp-server-policy/dhcpv6-server-policy/
ex3500-management-policy/ex3500-qos-class-map-policy/ex3500-qos-policy-map/exclude-devices/
```



```

firewall-policy/flag-unwritten-changes/guest-management-policy/hide-encrypted-values/
include-factory/interface/ip-access-list/ipv6-access-list/mac-access-list/management-
policy/
meshpoint/nsight-policy/profile/radio-qos-policy/rf-domain/roaming-assist-policy/rtl-
server-policy/
schedule-policy/smart-rf-policy/url-filter/url-list/web-filter-policy/wlan/wlan-qos-policy}
show running-config {aaa-policy/application-policy/association-acl-policy/auto-
provisioning-policy/
captive-portal-policy/database-client-policy/database-policy/dhcp-server-policy/dhcpv6-
server-policy/
ex3500-management-policy/ex3500-qos-class-map-policy/ex3500-qos-policy-map/guest-
management-policy/
firewall-policy/management-policy/nsight-policy/radio-qos-policy/roaming-assist-policy/rtl-
server-policy/
schedule-policy/smart-rf-policy/web-filter-policy/wlan-qos-policy}<POLICY-NAME> {include-
factory}
show running-config {flag-unwritten-changes}
show running-config {application <APPLICATION-NAME>/application-group <APPLICATION-GROUP-
NAME>}
show running-config exclude-devices
show running-config {device [<MAC>/self]} {include-factory}
show running-config {device-overrides {brief}}
show running-config {hide-encrypted-values {exclude-devices/include-factory}}
show running-config {include-factory}
show running-config {interface} {<INTERFACE-NAME>/ge/include-factory/me/port-channel/
pppoe1/vlan/wwan1}
show running-config {interface} {<INTERFACE-NAME>/ge <1-4>/include-factory/me1/
port-channel <1-2>/pppoe1/vlan <1-4094>/wwan1} {include-factory}
show running-config {ip-access-list <IP-ACCESS-LIST-NAME>/ipv6-access-list <IPv6-ACCESS-
LIST-NAME>/
mac-access-list <MAC-ACCESS-LIST-NAME>} {include-factory}
show running-config {meshpoint <MESHPOINT-NAME>} {include-factory}
show running-config {profile [anyap/ap6522/ap6562/ap71xx/ap7502/ap7522/ap7532/
ap7562/ap7602/ap7612/ap7622/ap7632/ap7662/ap81xx/ap8432/ap8533/rfs4000/nx5500/
nx75xx/nx9000/nx9600] <PROFILE-NAME>} {include-factory}
show running-config {rf-domain <DOMAIN-NAME>} {include-factory}
show running-config {wlan <WLAN-NAME>} {include-factory}
show running-config url-filter <URL-FILTER-NAME>
show running-config url-list <URL-LIST-NAME> {include-factory}

```

## Parameters

```

show running-config {flag-unwritten-changes}

```

running-config flag-unwritten-changes

Flags unsaved changes in the show > running-config command output. Optionally use the flag-unwritten-changes keyword to view changes that have been committed but not saved in the startup configuration. When used, all unsaved changes are marked with a “===” marker, as shown in the following show > running-config > flag-unwritten-changes output:

```
nx9500-6C8809(config)#show running-config flag-unwritten-changes
!
! Configuration of NX9500 version 5.9.2.0-017D
!
!
version 2.5
!
!
client-identity-group default
 load default-fingerprints
!
client-identity-group test2
 load default-fingerprints
!
===alias encrypted-string $WRITE 2 o5gA2zqj/q/
REWi8rTa7vQAAAAh4yAlYNBjqTVf4mMBsGA4i
!
===alias encrypted-string $enAlias2 2
JI4lPuMaCdMMx7rfBeyIAwAAAAoZ6tRlFfTlFXWvSicTMVZc
!
--More--
nx9500-6C8809(config)#
```

Execute the **write > memory** command to save these changes.

```
show running-config {aaa-policy/application-policy/association-acl-policy/
auto-provisioning-policy/captive-portal-policy/database-client-policy/database-policy/
dhcp-server-policy/dhcpv6-server-policy/ex3500-management-policy/ex3500-qos-class-map-
policy/
ex3500-qos-policy-map/guest-management-policy/firewall-policy/management-policy/nsight-
policy/
radio-qos-policy/roaming-assist-policy/rtl-server-policy/schedule-policy/smart-rf-policy/
web-filter-policy/wlan-qos-policy} <POLICY-NAME> {include-factory}
```

|                |                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| running-config | Displays current running configuration<br>Optionally, execute the command along with one of the associated keywords to view the running configuration for that top-level object. For example, to view a policy and its configuration, specify the policy type and provide the policy name.<br><br><b>Note:</b> If the command is executed without a keyword, the system displays the entire running configuration. |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                |                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <POLICY-TYPE><br><POLICY-NAME> | Optional. Select the policy type, for example, aaa-policy, auto-provisioning-policy, captive-portal-policy, etc. and then specify the policy name. The system displays the selected policy's configuration. <ul style="list-style-type: none"><li>• &lt;POLICY-NAME&gt; - Specify the name of the policy (should be existing and configured).</li></ul> |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                 |                                                                                                                                                          |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| include-factory | The following keyword is common to all policies: <ul style="list-style-type: none"><li>• include-factory - Optional. Includes factory defaults</li></ul> |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|

```
show running-config {device [<MAC>/self]} {include-factory}
```

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| running-config         | <p>Displays current running configuration</p> <p>Optionally, execute the command along with one of the associated keywords to view the running configuration for that top-level object. For example, to view a policy and its configuration, specify the policy type and provide the policy name.</p> <p><b>Note:</b> If the command is executed without a keyword, the system displays the entire running configuration.</p> |
| device<br>[<MAC> self] | <p>Optional. Displays device configuration</p> <ul style="list-style-type: none"> <li>• &lt;MAC&gt; – Displays a specified device configuration. Specify the MAC address of the device.</li> <li>• self – Displays the logged device's configuration</li> </ul>                                                                                                                                                               |
| include-factory        | <p>This keyword is common to all policies:</p> <ul style="list-style-type: none"> <li>• include-factory – Optional. Includes factory defaults</li> </ul>                                                                                                                                                                                                                                                                      |

```
show running-config {application <APPLICATION-NAME>/application-group <APPLICATION-GROUP-NAME>}
```

|                                               |                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| running-config                                | <p>Displays current running configuration</p> <p>Optionally, execute the command along with one of the associated keywords to view the running configuration for that top-level object. For example, to view a policy and its configuration, specify the policy type and provide the policy name.</p> <p><b>Note:</b> If the command is executed without a keyword, the system displays the entire running configuration.</p> |
| application <APPLICATION-NAME>                | <p>Displays an application's configuration. The application can be system-provided or user-defined.</p> <ul style="list-style-type: none"> <li>• &lt;APPLICATION-NAME&gt; – Specify the application name (should be existing).</li> </ul>                                                                                                                                                                                     |
| application-group<br><APPLICATION-GROUP-NAME> | <p>Displays an application-group's configuration</p> <ul style="list-style-type: none"> <li>• &lt;APPLICATION-GROUP-NAME&gt; – Specify the application-group name (should be existing and configured).</li> </ul>                                                                                                                                                                                                             |

```
show running-config {device [<MAC>|self]} {include-factory}
```

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| running-config      | <p>Displays current running configuration</p> <p>Optionally, execute the command along with one of the associated keywords to view the running configuration for that top-level object. For example, to view a policy and its configuration, specify the policy type and provide the policy name.</p> <p><b>Note:</b> If the command is executed without a keyword, the system displays the entire running configuration.</p> |
| device [<MAC> self] | <p>Optional. Displays device configuration</p> <ul style="list-style-type: none"> <li>• &lt;MAC&gt; – Displays a specified device configuration. Specify the MAC address of the device.</li> <li>• self – Displays the logged device's configuration</li> </ul>                                                                                                                                                               |
| include-factory     | <p>This keyword is common to all of the above keywords:</p> <ul style="list-style-type: none"> <li>• include-factory – Optional. Includes factory defaults</li> </ul>                                                                                                                                                                                                                                                         |

```
show running-config {hide-encrypted-values {exclude-devices/include-factory}}
```

|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| running-config                                          | Displays current running configuration<br>Optionally, execute the command along with one of the associated keywords to view the running configuration for that top-level object. For example, to view a policy and its configuration, specify the policy type and provide the policy name.<br><br><b>Note:</b> If the command is executed without a keyword, the system displays the entire running configuration. |
| hide-encrypted-values {exclude-devices include-factory} | Optional. Replaces all encrypted passwords with the standard characters ***** in the <b>show &gt; running-config</b> output <ul style="list-style-type: none"> <li>exclude-devices – Optional. Excludes devices from the running configuration displayed</li> <li>include-factory – Optional. Includes factory default values in the running configuration displayed</li> </ul>                                    |

`show running-config {device-overrides {brief}}`

|                        |                                                                                                                                                                                     |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| running-config         | Displays current running configuration                                                                                                                                              |
| device-overrides brief | Optional. Displays overrides applied at the device's configuration <ul style="list-style-type: none"> <li>brief – Optional. Displays a brief summary of device overrides</li> </ul> |

`show running-config {exclude-devices}`

|                 |                                                                                          |
|-----------------|------------------------------------------------------------------------------------------|
| running-config  | Displays current running configuration                                                   |
| exclude-devices | Optional. Excludes device configuration details from the running configuration displayed |

`show running-config {include-factory}`

|                 |                                        |
|-----------------|----------------------------------------|
| running-config  | Displays current running configuration |
| include-factory | Optional. Includes factory defaults    |

`show running-config {interface} {<INTERFACE-NAME>/ge <1-4>/include-factory/  
me1/port-channel <1-2>/pppoe1/vlan <1-4094>/wwan1} {include-factory}`

|                    |                                                                                                                                                                                    |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| running-config     | Displays current running configuration                                                                                                                                             |
| interface          | Optional. Displays interface configuration                                                                                                                                         |
| <INTERFACE-NAME>   | Optional. Displays a specified interface configuration. Specify the interface name.                                                                                                |
| ge <1-4>           | Optional. Displays GigabitEthernet interface configuration <ul style="list-style-type: none"> <li>&lt;1-4&gt; – Specify the GigabitEthernet interface index from 1 - 4.</li> </ul> |
| me1                | Optional. Displays FastEthernet interface configuration                                                                                                                            |
| port-channel <1-2> | Optional. Displays port channel interface configuration <ul style="list-style-type: none"> <li>&lt;1-2&gt; – Specify the port channel interface index from 1 - 2.</li> </ul>       |
| pppoe1             | Optional. Displays PPP over Ethernet interface configuration                                                                                                                       |
| vlan <1-4094>      | Displays VLAN interface configuration <ul style="list-style-type: none"> <li>&lt;1-4094&gt; – Specify the VLAN interface number from 1 - 4094.</li> </ul>                          |

|                 |                                                                                                                                                            |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wwan1           | Optional. Displays Wireless WAN interface configuration                                                                                                    |
| include-factory | The following keyword is common to all interfaces: <ul style="list-style-type: none"> <li>include-factory - Optional. Includes factory defaults</li> </ul> |

```
show running-config {ip-access-list <IP-ACCESS-LIST-NAME>/ipv6-access-list
<IPv6-ACCESS-LIST-NAME>/mac-access-list <MAC-ACCESS-LIST-NAME> {include-factory}}
```

|                                      |                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| running-config                       | Displays current running configuration<br>Optionally, execute the command along with one of the associated keywords to view the running configuration for that top-level object. For example, to view a policy and its configuration, specify the policy type and provide the policy name.<br><br><b>Note:</b> If the command is executed without a keyword, the system displays the entire running configuration. |
| ip-access-list <IP-ACCESS-LIST-NAME> | Optional. Displays IP access list configuration <ul style="list-style-type: none"> <li>&lt;IP-ACCESS-LIST-NAME&gt; - Specify the IP access list name</li> </ul>                                                                                                                                                                                                                                                    |
| <ACL-TYPE> <IP/IPv6/MAC-ACL-NAME>    | Optional. Select the ACL type, for example, ip-access-list, ipv6-access-list, or mac-access-list, and then specify the ACL name. The system displays the selected ACL's configuration. <ul style="list-style-type: none"> <li>&lt;IP/IPv6/MAC-ACL-NAME&gt; - Specify the name of the ACL (should be existing and configured).</li> </ul>                                                                           |
| include-factory                      | The following keyword is common to the 'ip-access-list' and 'mac-access-list' parameters: <ul style="list-style-type: none"> <li>include-factory - Optional. Includes factory defaults</li> </ul>                                                                                                                                                                                                                  |

```
show running-config {meshpoint <MESHPOINT-NAME>} {include-factory}
```

|                            |                                                                                                                                                  |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| running-config             | Displays current running configuration                                                                                                           |
| meshpoint <MESHPOINT-NAME> | Optional. Displays meshpoint configuration <ul style="list-style-type: none"> <li>&lt;MESHPOINT-NAME&gt; - Specify the meshpoint name</li> </ul> |
| include-factory            | Optional. Includes factory defaults along with running configuration details                                                                     |

```
show running-config {profile [anyap/ap6522/ap6562/ap71xx/ap7502/ap7522/ap7532/
ap7562/ap7602/ap7612/ap7622/ap7632/ap7662/ap81xx/ap8432/ap8533/rfs4000/nx5500/nx75xx/
nx9000/nx9600] <PROFILE-NAME>} {include-factory}
```

|                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| running-config                       | Displays current running configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| profile <DEVICE-TYPE> <PROFILE-NAME> | Optional. Displays current configuration for a specified profile. Select the device type, and then specify the profile name. <ul style="list-style-type: none"> <li>&lt;DEVICE-TYPE&gt; - Select the device type. The options are: AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533, RFS 4000, NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000.</li> <li>&lt;PROFILE-NAME&gt; - Specify the profile name for the selected &lt;DEVICE-TYPE&gt;.</li> </ul> <b>Note:</b> Select the 'anyap' option to view the running configuration of any type of device. |
| include-factory                      | Optional. This parameter is common to all profiles. When selected, it includes factory defaults in the output.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

```
show running-config {rf-domain <DOMAIN-NAME>} {include-factory}
```

|                         |                                                                                                                                                                                                                          |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| running-config          | Displays current running configuration                                                                                                                                                                                   |
| rf-domain <DOMAIN-NAME> | Optional. Displays current configuration for a RF Domain <ul style="list-style-type: none"> <li>• &lt;DOMAIN-NAME&gt; - Displays current configuration for a specified RF Domain. Specify the RF Domain name.</li> </ul> |
| include-factory         | Optional. Includes factory defaults                                                                                                                                                                                      |

```
show running-config {wlan <WLAN-NAME>}{include-factory}
```

|                  |                                                                                                                                                                                                         |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| running-config   | Displays current running configuration                                                                                                                                                                  |
| wlan <WLAN-NAME> | Optional. Displays current configuration for a WLAN <ul style="list-style-type: none"> <li>• &lt;WLAN-NAME&gt; - Displays current configuration for a specified WLAN. Specify the WLAN name.</li> </ul> |
| include-factory  | Optional. Includes factory defaults                                                                                                                                                                     |

```
show running-config url-filter <URL-FILTER-NAME>
```

|                              |                                                                                                                                                                                                                      |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| running-config               | Displays current running configuration                                                                                                                                                                               |
| url-filter <URL-FILTER-NAME> | Optional. Displays current configuration for the URL filter identified by the <URL-FILTER-NAME> keyword <ul style="list-style-type: none"> <li>• &lt;URL-FILTER-NAME&gt; - Specify the URL filter's name.</li> </ul> |

```
show running-config url-list <URL-LIST-NAME> {include-factory}
```

|                          |                                                                                                                                                                                                              |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| running-config           | Displays current running configuration                                                                                                                                                                       |
| url-list <URL-LIST-NAME> | Optional. Displays current configuration for the URL list identified by the <URL-LIST-NAME> keyword <ul style="list-style-type: none"> <li>• &lt;URL-LIST-NAME&gt; - Specify the URL list's name.</li> </ul> |
| include-factory          | Optional. Includes factory defaults                                                                                                                                                                          |

## Examples

```
nx9500-6C8809#show running-config device self
!
version 2.5
!
!
ip snmp-access-list default
 permit any
!
firewall-policy default
 no ip dos tcp-sequence-past-window
!
!
mint-policy global-default
!
!
management-policy default
 no telnet
 no http server
 https server
 no ftp
 ssh
 user admin password 1 fd07f19c6caf46e5b7963a802d422a708ad39a24906e04667c8642299c8462f1
```

```

role superuser access all
--More--
nx9500-6C8809#
nx9500-6C8809#show running-config profile ap8432 default-ap8432
profile ap8432 default-ap8432
 autoinstall configuration
 autoinstall firmware
 crypto ikev1 policy ikev1-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 crypto load-management
 crypto remote-vpn-client
 interface radiol
 interface radio2
 interface bluetooth1
 shutdown
 interface ge1
 interface ge2
 interface vlan1
--More--
nx9500-6C8809#
nx9500-6C8809#show running-config url-filter URL_FILTER_Shopping include-factory
url-filter URL_FILTER_Shopping
 no description
 blacklist category-type p2p precedence 20 description description
 blacklist category-type news-sports-general category shopping precedence 10 description
 description
 blockpage path internal
 blockpage internal org-name Your Organization Name
 blockpage internal org-signature Your Organization Name, All Rights Reserved.
 blockpage internal title This URL may have been filtered.
 blockpage internal header The requested URL could not be retrieved.
 blockpage internal footer If you have any questions please contact your IT department.
 blockpage internal content The site you have attempted to reach may be considered
 inappropriate for access.
 no blockpage internal main-logo
 no blockpage internal small-logo
 no blockpage external
nx9500-6C8809#
nx9500-6C8809#show running-config url-list AllowedShopping
url-list AllowedShopping
 url ebay.com depth 10
 url amazon.com depth 10
nx9500-6C8809#
nx9500-6C8809#show running-config application Bing
application Bing
 app-category streaming
 use url-list Bing
nx9500-6C8809#
nx9500-6C8809#sho running-config application-group amazon
application-group amazon
 application amazon_cloud
 application amazon_shop
 application amazon-prime-music
 application amazon-prime-video
nx9500-6C8809#

```

## session-changes

Displays configuration changes made in the current session

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show session-changes
```

### Parameters

None

### Examples

```
nx9500-6C8809#show session-changes
```

```
No changes in this session
```

```
nx9500-6C8809#
```

## session-config

Lists active open sessions on a device

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show session-config {exclude-devices|include-factory}
```

### Parameters

```
show session-config {exclude-devices|include-factory}
```

|                                                  |                                                                                                                                                                                                                                            |
|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| session-config {exclude-devices include-factory} | Displays current session configuration <ul style="list-style-type: none"><li>• exclude-devices - Optional. Excludes device configuration details from the output</li><li>• include-factory - Optional. Includes factory defaults</li></ul> |
|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config)#show session-config
!
! Configuration of NX9500 version 5.9.2.0-017D
!
!
version 2.5
!
```



```

!
client-identity-group default
 load default-fingerprints
!
ip access-list BROADCAST-MULTICAST-CONTROL
 permit tcp any any rule-precedence 10 rule-description "permit all TCP traffic"
 permit udp any eq 67 any eq dhcp rule-precedence 11 rule-description "permit DHCP
replies"
 deny udp any range 137 138 any range 137 138 rule-precedence 20 rule-description "deny
windows netbios"
 deny ip any 224.0.0.0/4 rule-precedence 21 rule-description "deny IP multicast"
 deny ip any host 255.255.255.255 rule-precedence 22 rule-description "deny IP local
broadcast"
 permit ip any any rule-precedence 100 rule-description "permit all IP traffic"
!
mac access-list PERMIT-ARP-AND-IPv4
 permit any any type ip rule-precedence 10 rule-description "permit all IPv4 tra
--More--
nx9500-6C8809(config)#

```

## sessions

Displays CLI sessions initiated on a device

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show sessions all {on <DEVICE-NAME>}
```

### Parameters

```
show sessions all {on <DEVICE-NAME>}
```

|                  |                                                                                                                                                                                                                                                                          |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| sessions         | Displays CLI sessions initiated on a device                                                                                                                                                                                                                              |
| all              | Displays all sessions including internal                                                                                                                                                                                                                                 |
| on <DEVICE-NAME> | Optional. This is a recurring keyword and is common to the 'all' parameter. Displays CLI sessions on a specified device. <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

### Examples

```

nx9500-6C8809#show sessions
INDEX COOKIE NAME START TIME FROM ROLE
1 2 snmp 2018-02-02 08:39:28 127.0.0.1 superuser
2 3 snmp2 2018-02-02 08:39:28 127.0.0.1 superuser
3 53 admin 2018-02-09 14:43:19 134.141.244.24 superuser

nx9500-6C8809#

```

## site-config-diff

Displays the difference in site configuration available on the NOC and a site.

The WiNG HM network defines a three-tier structure, consisting of multiple wireless sites managed by a single NOC controller, The NOC controller constitutes the first and the site controllers constitute the second tier of the hierarchy. The site controllers may or may not be grouped to form clusters. The site controllers in turn adopt and manage Access Points that form the third tier of the hierarchy.

NOC controllers possess default site configuration details. Overrides applied at the site level result in a mismatch of configuration at the site and the default site configuration available on the NOC controller. Use this command to view this difference.

**Supported in the following platforms:**

- Wireless Controllers – RFS 4000
- Service Platforms – NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000



**Note**

This command returns an output only when executed on a NOC controller.

**Syntax**

```
show site-config-diff <SITE-NAME>
```

**Parameters**

```
show site-config-diff <SITE-NAME>
```

|                              |                                                                                              |
|------------------------------|----------------------------------------------------------------------------------------------|
| site-config-diff <SITE-NAME> | Displays the configuration difference for the specified site                                 |
|                              | <ul style="list-style-type: none"><li>• &lt;SITE-NAME&gt; – Specify the site name.</li></ul> |

**Examples**

```
nx9500-6C8809#show site-config-diff 5C-0E-8B-18-06-F4
---- Config diff for switch 5C-0E-8B-18-06-F4 ----
rfs4000 5C-0E-8B-18-06-F4
interface pppoe1
 no shutdown
nx9500-6C8809#
```

*smart-rf*

Displays Smart RF (Self-Monitoring At Run Time RF) statistical history to assess adjustments made to device configurations to compensate for detected coverage holes or device failures

When invoked by an administrator, Smart RF instructs access point radios to change to a specific channel and begin beaconing using the maximum available transmit power. Within a well-planned deployment, any RF Domain member access point radio should be reachable by at least one other radio. Smart RF records signals received from its neighbors as well as signals from external, un-managed radios. AP-to-AP distance is recorded in terms of signal attenuation. The information from external radios is used during channel assignment to minimize interference.

**Supported in the following platforms:**

- Access Points – AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers – RFS 4000
- Service Platforms – NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000



## Syntax

```
show smart-rf [ap|channel-distribution|history|history-timeline|interfering-ap|
interfering-neighbors|radio|select-shutdown]
show smart-rf ap {<MAC>|<DEVICE-NAME>} /activity/energy/neighbors/on <DOMAIN-NAME>}
show smart-rf ap {<MAC>|<DEVICE-NAME>} {on <DOMAIN-NAME>}
show smart-rf ap (activity|energy|neighbors) [<MAC>|<DEVICE-NAME>] {(on <DOMAIN-NAME>)}
show smart-rf [channel-distribution|history|history-timeline] {on <DOMAIN-NAME>}
show smart-rf radio {<MAC>|activity/all-11an/all-11bgn/channel/energy/neighbors|
on <DOMAIN-NAME>}
show smart-rf radio {<MAC>|all-11an/all-11bgn/energy <MAC>} {on <DOMAIN-NAME>}
show smart-rf radio {activity|neighbors} {<MAC>|all-11an/all-11bgn} {on <DOMAIN-NAME>}
show smart-rf interfering-ap {<MAC>|<DEVICE-NAME>} /on <DOMAIN-NAME>}
show smart-rf interfering-neighbors {<MAC>|<DEVICE-NAME>} /on <DOMAIN-NAME>} /
threshold <50-100>}
show smart-rf select-shutdown {AP-MAC|<AP-DEVICE-NAME>} /on <RF-DOMAIN-NAME>}
```

## Parameters

```
show smart-rf ap {<MAC>|<DEVICE-NAME>} {on <DOMAIN-NAME>}
```

|                  |                                                                                                                                                                 |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| smart-rf         | Displays Smart RF related information                                                                                                                           |
| ap               | Displays access point related Smart RF information                                                                                                              |
| <MAC>            | Optional. Uses MAC addresses to identify access points. Displays all access points, if no MAC address is specified.                                             |
| <DEVICE-NAME>    | Optional. Uses an administrator defined name to identify an access point                                                                                        |
| on <DOMAIN-NAME> | Optional. Displays access point details on a specified RF Domain <ul style="list-style-type: none"><li>&lt;DOMAIN-NAME&gt; - Specify the domain name.</li></ul> |

```
show smart-rf ap (activity|energy|neighbors) [<MAC>|<DEVICE-NAME>] {(on <DOMAIN-NAME>)}
```

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| smart-rf | Displays Smart RF related information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| ap       | Displays AP related Smart RF information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| activity | Optional. Displays Smart RF activity related information<br>Use this option to view the following: <ul style="list-style-type: none"><li>Time-period - Lists the frequency Smart RF activity is trended for the RF Domain. Trending periods include the current hour, last 24 hours, or the last seven days. Comparing Smart RF adjustments versus the last seven days enables an administrator to assess whether periods of interference and poor performance were relegated to just specific periods.</li><li>Power changes - Displays the number of Smart RF initiated power level changes needed for RF Domain member devices during each of the three trending periods. Determine whether power compensations were relegated to known device outages or if compensations were consistent over the course of a day or week.</li><li>Channel changes - Lists the number of Smart RF initiated channel changes needed for RF Domain member devices during each of the three trending periods. Determine if channel adjustments were relegated to known device count increases or decreases over the course of a day or week.</li><li>Coverage changes - Displays the number of Smart RF initiated coverage changes needed for RF Domain member devices during each of the three trending periods. Determine if coverage changes were relegated to known device failures or known periods of interference over the course of a day or week.</li></ul> |

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| energy                 | Optional. Displays AP energy for a specified AP or all APs<br>Use this option to view an RF Domain member access point's operating channels, noise level and neighbor count. This information helps assess whether Smart RF neighbor recovery is needed in respect to poorly performing access points.                                                                                                                           |
| neighbors              | Optional. Displays AP neighbors<br>Use this option to view attributes of neighbor radio resources available for Smart RF radio compensations for other RF Domain member device radios.                                                                                                                                                                                                                                           |
| {<MAC>  <DEVICE-NAME>} | The following keywords are common to all of the above parameters: <ul style="list-style-type: none"> <li>• &lt;MAC&gt; - Displays all of the above mentioned information for a specified AP, identified by its MAC address. Specify the AP's MAC address.</li> <li>• &lt;DEVICE-NAME&gt; - Displays all of the above mentioned information for a specified AP, identified by its hostname. Specify the AP's hostname.</li> </ul> |
| on <DOMAIN-NAME>       | Optional. Displays Access Point details on a specified RF Domain. <ul style="list-style-type: none"> <li>• &lt;DOMAIN-NAME&gt; - Specify the domain name.</li> </ul>                                                                                                                                                                                                                                                             |

```
show smart-rf [channel-distribution|history|history-timeline] {on <DOMAIN-NAME>}
```

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| smart-rf             | Displays Smart RF related information                                                                                                                                                                                                                                                                                                                                                                           |
| channel-distribution | Displays Smart RF channel distribution information. This provides an overview of how RF Domain member devices are utilizing different channels to optimally support connect devices and avoid congestion and interference with neighboring devices. Assess whether the channel spectrum is being effectively utilized and whether channel changes are warranted to improve RF Domain member device performance. |
| history              | Displays Smart RF calibration history<br>Use this option to view description and types of Smart RF events impacting RF Domain member devices.                                                                                                                                                                                                                                                                   |
| history-timeline     | Displays extended Smart RF calibration history on an hourly or daily timeline<br>Use this option to view the time stamp when Smart RF status was updated on behalf of a Smart RF adjustment within the selected RF Domain.                                                                                                                                                                                      |
| on <DOMAIN-NAME>     | This parameter is common to all of above smart RF options: <ul style="list-style-type: none"> <li>• on &lt;DOMAIN-NAME&gt; - Optional. Displays Smart RF configuration, based on the parameters passed, on a specified RF Domain</li> <li>• on &lt;DOMAIN-NAME&gt; - Specify the RF Domain name.</li> </ul>                                                                                                     |

```
show smart-rf radio {<MAC>|all-11an|all-11bgn|energy <MAC>} {on <DOMAIN-NAME>}
```

|           |                                                                                                                   |
|-----------|-------------------------------------------------------------------------------------------------------------------|
| smart-rf  | Displays Smart RF related information                                                                             |
| radio     | Displays radio related commands                                                                                   |
| <MAC>     | Optional. Displays details of a specified radio. Specify the radio's MAC address in the AA-BB-CC-DD-EE-FF format. |
| all-11an  | Optional. Displays all 11a radios currently in the configuration                                                  |
| all-11bgn | Optional. Displays all 11bg radios currently in the configuration                                                 |

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| energy {<MAC>}   | Optional. Displays radio energy<br>Specify the MAC address of the radio <ul style="list-style-type: none"> <li>• &lt;MAC&gt; - Optional. Specify the radio's MAC address in the AA-BB-CC-DD-EE-FF format.</li> </ul> <p>Use this option to view an RF Domain member access point radio's operating channel, noise level and neighbor count. This information helps assess whether Smart RF neighbor recovery is needed in respect to poorly performing radios.</p> |
| on <DOMAIN-NAME> | The following keyword is common to all of the above parameters: <ul style="list-style-type: none"> <li>• on &lt;DOMAIN-NAME&gt; - Optional. Displays radio details on a specified RF Domain</li> <li>• &lt;DOMAIN-NAME&gt; - Specify the RF Domain name.</li> </ul>                                                                                                                                                                                                |

```
show smart-rf radio {activity/neighbors} {<MAC>/all-11a/all-11bgn} {on <DOMAIN-NAME>}
```

|                  |                                                                                                                                                                                    |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| smart-rf         | Displays Smart RF related information                                                                                                                                              |
| radio            | Displays radio related commands                                                                                                                                                    |
| activity         | Optional. Displays changes related to radio power, number of radio channels, or coverage holes. Use additional filters to view specific details.                                   |
| <MAC>            | Optional. Displays radio activity for a specified radio <ul style="list-style-type: none"> <li>• &lt;MAC&gt; - Specify the radio's MAC address.</li> </ul>                         |
| all-11a          | Optional. Displays radio activity of all 11a radios in the configuration                                                                                                           |
| all-11bgn        | Optional. Displays radio activity of all 11bgn radios in the configuration                                                                                                         |
| on <DOMAIN-NAME> | Optional. Displays radio activity of all radios within a specified RF Domain <ul style="list-style-type: none"> <li>• &lt;DOMAIN-NAME&gt; - Specify the RF Domain name.</li> </ul> |

```
show smart-rf interfering-ap {<MAC>/<DEVICE-NAME>/on <DOMAIN-NAME>}
```

|                  |                                                                                                                                                                                                                                                     |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| smart-rf         | Displays Smart RF related information                                                                                                                                                                                                               |
| interfering-ap   | Displays interfering access points (requiring potential isolation) information                                                                                                                                                                      |
| <MAC>            | Optional. Displays information of a specified interfering access point <ul style="list-style-type: none"> <li>• &lt;MAC&gt; - Specify the Access Point's MAC address.</li> </ul> <p><b>Note:</b> Considers all APs if this parameter is omitted</p> |
| <DEVICE-NAME>    | Optional. Displays interfering Access Point information on a specified device <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; - Specify the device name.</li> </ul> <p><b>Note:</b> Considers all APs if this parameter is omitted</p> |
| on <DOMAIN-NAME> | Optional. Displays all interfering Access Point information within a specified RF Domain <ul style="list-style-type: none"> <li>• &lt;DOMAIN-NAME&gt; - Specify the RF Domain name.</li> </ul>                                                      |

```
show smart-rf interfering-neighbors {<MAC>/<DEVICE-NAME>/on <DOMAIN-NAME>/threshold <50-100>}
```

|                |                                                           |
|----------------|-----------------------------------------------------------|
| smart-rf       | Displays Smart RF related information                     |
| interfering-ap | Displays interfering neighboring Access Point information |

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <MAC>              | Optional. Displays interfering neighboring Access Point information <ul style="list-style-type: none"> <li>• &lt;MAC&gt; - Specify the Access Point's MAC address.</li> </ul> <p><b>Note:</b> Considers all APs if this parameter is omitted</p>                                                                                                                                                                                                                                              |
| <DEVICE-NAME>      | Optional. Displays all interfering neighboring Access Point information on a specified device <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; - Specify the device name.</li> </ul> <p><b>Note:</b> Considers all APs if this parameter is omitted</p>                                                                                                                                                                                                                           |
| threshold <50-100> | Optional. Specifies the maximum attenuation threshold of interfering neighbors <ul style="list-style-type: none"> <li>• &lt;50-100&gt; - Specify a value from 50 -100 dB.</li> </ul> <p>Attenuation is a measure of the reduction of signal strength during transmission. Attenuation is the opposite of amplification, and is normal when a signal is sent from one point to another. If the signal attenuates too much, it becomes unintelligible. Attenuation is measured in decibels.</p> |
| on <DOMAIN-NAME>   | Optional. Displays radio activity of all radios within a specified RF Domain <ul style="list-style-type: none"> <li>• &lt;DOMAIN-NAME&gt; - Specify the RF Domain name.</li> </ul>                                                                                                                                                                                                                                                                                                            |

```
show smart-rf select-shutdown {AP-MAC/<AP-DEVICE-NAME>/on <RF-DOMAIN-NAME>}
```

|                     |                                                                                                                                                                                                                                                                                                            |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| smart-rf            | Displays Smart RF related information                                                                                                                                                                                                                                                                      |
| select-shutdown     | Displays 2.4 GHz APs shutdown to maintain co-channel interference (CCI) levels within specified limits. Note, this information is displayed only if select-shutdown is enabled in the smart-rf policy context. For more information, see <a href="#">select-shutdown</a> on page 1643.                     |
| <AP-MAC>            | Optional. Displays if a specified AP, identified by its MAC address, was shutdown as part of the select-shutdown feature. <ul style="list-style-type: none"> <li>• &lt;AP-MAC&gt; - Specify the access point's MAC address.</li> </ul> <p><b>Note:</b> Considers all APs if this parameter is omitted.</p> |
| <AP-DEVICE-NAME>    | Optional. Displays if a specified AP, identified by its device name, was shutdown as part of the select-shutdown feature. <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; - Specify the AP's device name.</li> </ul> <p><b>Note:</b> Considers all APs if this parameter is omitted.</p>      |
| on <RF-DOMAIN-NAME> | Optional. Displays APs, within a specified RF Domain, that were shutdown as part of the select-shutdown feature. <ul style="list-style-type: none"> <li>• &lt;RF-DOMAIN-NAME&gt; - Specify the RF Domain name.</li> </ul>                                                                                  |

## Examples

```
nx9500-6C8809(config)#show smart-rf calibration-status
No calibration currently in progress
nx9500-6C8809(config)#
rfs4000-22E006#show smart-rf select-shutdown
```

```

```

| RADIO            | RADIO-MAC         | STATE  |
|------------------|-------------------|--------|
| ap7532-15E868:R1 | FC-0A-81-A3-27-60 | On     |
| ap7532-82C614:R1 | 84-24-8D-93-E7-D0 | On     |
| ap7532-15E54C:R1 | FC-0A-81-A3-1A-90 | Hidden |

```

```

|                  |                   |        |
|------------------|-------------------|--------|
| ap7522-189548:R1 | 84-24-8D-2C-02-C0 | On     |
| ap7522-847CC8:R1 | 84-24-8D-9F-F3-B0 | On     |
| ap7532-1601A4:R1 | FC-0A-81-A3-14-A0 | Hidden |

-----  
rfs4000-22E006#

## spanning-tree

Displays spanning tree utilization information

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show spanning-tree mst {configuration/detail/instance/on}
show spanning-tree mst {configuration} {(on <DEVICE-NAME>)}
show spanning-tree mst {detail} {interface/on}
show spanning-tree mst {detail} interface {<INTERFACE-NAME>/ge <1-4>/me1/
port-channel <1-2>/pppoe1/vlan <1-4094>/wwan1} {(on <DEVICE-NAME>)}
show spanning-tree mst {instance <1-15>} {interface <INTERFACE-NAME>} {(on <DEVICE-NAME>)}
```

### Parameters

```
show spanning-tree mst {configuration} {(on <DEVICE-NAME>)}
```

|                                  |                                                                                                                                                                                                                                                                                    |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| spanning-tree                    | Displays spanning tree utilization information                                                                                                                                                                                                                                     |
| mst                              | Displays MST (Multiple Spanning Tree) related information                                                                                                                                                                                                                          |
| configuration {on <DEVICE-NAME>} | Optional. Displays MST configuration <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; - Optional. Displays MST configuration on a specified device</li> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP,wireless controller, or service platform.</li> </ul> |

```
show spanning-tree mst {detail} interface {<INTERFACE-NAME>/ge <1-4>/me1/
port-channel <1-2>/pppoe1/vlan <1-4094>/wwan1} {(on <DEVICE-NAME>)}
```

|               |                                                                               |
|---------------|-------------------------------------------------------------------------------|
| spanning-tree | Displays spanning tree information                                            |
| mst           | Displays MST configuration                                                    |
| detail        | Optional. Displays detailed MST configuration, based on the parameters passed |

|                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| interface<br>[<INTERFACE>] age<br><1-4> me  port-<br>channel <1-2> <br>pppoe  vlan<br><1-4094> wwan] | <p>Displays detailed MST configuration for a specified interface</p> <ul style="list-style-type: none"> <li>• &lt;INTERFACE&gt; – Displays detailed MST configuration for a specified interface. Specify the interface name.</li> <li>• age &lt;1-4&gt; – Displays GigabitEthernet interface MST configuration <ul style="list-style-type: none"> <li>• &lt;1-4&gt; – Select the GigabitEthernet interface index from 1 - 4.</li> </ul> </li> <li>• me1 – Displays FastEthernet interface MST configuration</li> <li>• port-channel – Displays port channel interface MST configuration <ul style="list-style-type: none"> <li>• &lt;1-2&gt; – Select the port channel interface index from 1 - 2.</li> </ul> </li> <li>• pppoe1 – Displays PPP over Ethernet interface MST configuration</li> <li>• vlan – Displays VLAN interface MST configuration <ul style="list-style-type: none"> <li>• &lt;1-4094&gt; – Select the SVI VLAN ID from 1 - 4094.</li> </ul> </li> <li>• wwan1 – Displays Wireless WAN interface MST configuration</li> </ul> |
| on <DEVICE-NAME>                                                                                     | <p>The following keyword is common to all interfaces:<br/>Optional. Displays detailed MST configuration on a specified device</p> <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

```
show spanning-tree mst {instance <1-15>} {interface <INTERFACE-NAME>} {(on <DEVICE-NAME>)}
```

|                            |                                                                                                                                                                                                                                                                |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| spanning-tree              | Displays spanning tree information                                                                                                                                                                                                                             |
| mst                        | Displays MST configuration. Use additional filters to view specific details.                                                                                                                                                                                   |
| instance <1-15>            | <p>Optional. Displays information for a particular MST instance</p> <ul style="list-style-type: none"> <li>• &lt;1-15&gt; – Specify the instance ID from 1 - 15.</li> </ul>                                                                                    |
| interface <INTERFACE-NAME> | <p>Optional. Displays MST configuration for a specific interface instance. The options are:</p> <ul style="list-style-type: none"> <li>• &lt;INTERFACE-NAME&gt; – Displays MST configuration for a specified interface. Specify the interface name.</li> </ul> |
| on <DEVICE-NAME>           | <p>Optional. Displays MST configuration on a specified device</p> <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul>                                              |

## Examples

```
nx9500-6C8809#show spanning-tree mst configuration
```

```
%%
% MSTP Configuration Information for bridge 1 :
%-----
% Format Id : 0
% Name : My Name
% Revision Level : 0
% Digest : 0xac36177f50283cd4b83821d8ab26de62
%-----
%%
```

```
nx9500-6C8809#
```

```
nx9500-6C8809#show spanning-tree mst detail interface ge 1
% Bridge up - Spanning Tree Disabled
% CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% Forward Delay 15 - Hello Time 2 - Max Age 20 - Max hops 20
% 1: CIST Root Id 800000157081742e
% 1: CIST Reg Root Id 800000157081742e
% 1: CIST Bridge Id 800000157081742e
% portfast bpdu-filter disabled
% portfast bpdu-guard disabled
% portfast portfast errdisable timeout disabled
```



```

% portfast errdisable timeout interval 300 sec
% cisco interoperability not configured - Current cisco interoperability off

% gel: Port 2001 - Id 87d1 - Role Disabled - State Forwarding
% gel: Designated External Path Cost 0 - Internal Path Cost 0
%
--More--
nx9500-6C8809#

```

### startup-config

Displays complete startup configuration script

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
show startup-config {include-factory}
```

#### Parameters

```
show startup-config {include-factory}
```

|                                |                                                                                                                                                 |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| startup-config include-factory | Displays startup configuration script <ul style="list-style-type: none"> <li>• include-factory - Optional. Includes factory defaults</li> </ul> |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```

nx9500-6C8809#show startup-config
!
! Configuration of NX9500 version 5.9.2.0-017D
!
!
version 2.5
!
password-encryption-version 1.0
inline-password-encryption
password-encryption-key secret 2
2cd258b63fa0e16a753394d779cbc5a20000002065d2c29edf373ed42131fa410426d5cb8b0296ffea49331cb72
e122e421acc9c
!
client-identity-group default
 load default-fingerprints
!
client-identity-group test2
 load default-fingerprints
!
alias network-group $NetGrpAlias address-range 192.168.13.7 to 192.168.13.16 192.168.13.20
to 192.168.13.25
alias network-group $NetGrpAlias network 192.168.13.0/24 192.168.16.0/24
!
alias network $NetworkAlias 192.168.13.0/24
!
--More--
nx9500-6C8809#

```

Displays adopted T5 controller statistics



#### Note

This command is applicable only on WiNG controllers with adopted and managed T5 controllers.

#### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
show t5 [boot|clock|cpe|interface|mac|system|temperature|uptime|version|
wireless] {on <T5-DEVICE-NAME>}
show t5 [boot|clock|system|temperature|uptime|version] {on <T5-DEVICE-NAME>}
show t5 cpe [address|boot|ether port status|led|reset|system|uptime|version]
{on <T5-DEVICE-NAME>}
show t5 interface [dsl|fe|ge|radio]
show t5 interface [dsl|fe|ge] [counter|description|errors|status|utilization]
{on <T5-DEVICE-NAME>}
show t5 interface dsl custom [avg|dses|dsses|peak|uses|usses] {on <T5-DEVICE-NAME>}
show t5 interface radio [stats|status|wlan-map] {on <T5-DEVICE-NAME>}
show t5 mac table [filter name [dsl<1-24>|ge <1-2>|vlan <1-4094>|wlan <1-24>]
{on <T5-DEVICE-NAME>}
show t5 wireless [client|wlan]
show t5 wireless client {filter name [association-status/authentication-status/bss/
mac-address/retry-percentage/rssi-value]} {on <T5-DEVICE-NAME>}
show t5 wireless wlan counters [qos|rate|size] {on <T5-DEVICE-NAME>}
```

#### Parameters

```
show t5 [boot|clock|system|temperature|uptime|version] {on <T5-DEVICE-NAME>}
```

|                     |                                                                                                                                                                                                                                         |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| t5                  | Displays adopted T5 controller statistics                                                                                                                                                                                               |
| boot                | Displays the T5 device's boot details. Use this option to view the primary and secondary image files available to use for booting up.                                                                                                   |
| clock               | Displays the T5 controller's system time, as reported from the controller itself or its remote NTP time resource                                                                                                                        |
| system              | Displays T5 controller's system information, which includes the T5 controller's hostname, MAC address, RF Domain, system clock, uptime                                                                                                  |
| temperature         | Displays T5 controller's current temperature                                                                                                                                                                                            |
| uptime              | Displays the T5 controller's uptime (the time it has been actively deployed and operational)                                                                                                                                            |
| version             | Displays the T5 controller's primary and secondary firmware images                                                                                                                                                                      |
| on <T5-DEVICE-NAME> | Optional. Executes the command on a specified T5 device <ul style="list-style-type: none"> <li>• &lt;T5-DEVICE-NAME&gt; - Specify the T5 device's hostname. An error message is displayed if no T5 device name is specified.</li> </ul> |

```
show t5 cpe [address|boot|ether port status|led|reset|system|uptime|version]
{on <T5-DEVICE-NAME>}
```

|                     |                                                                                                                                                                                                                                                      |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| t5                  | Displays adopted T5 controller statistics                                                                                                                                                                                                            |
| cpe                 | Displays the T5 controller managed CPE (Customer Premises Equipment) statistics based on the parameters passed. Use this command to verify each CPE address credentials and whether currently disconnected or ready for radio coverage area support. |
| address             | Displays each linked CPE's current IP address used as its network identifier                                                                                                                                                                         |
| boot                | Displays the primary and secondary firmware versions available to each CPE, along with status of the most recent upgrade operation details                                                                                                           |
| ether port status   | Displays Ethernet port status                                                                                                                                                                                                                        |
| led                 | Displays whether the CPEs currently have their LEDs enabled or disabled. In places like hospitals, its not uncommon for access points to be operational, but their LEDs off as to not disturb patients.                                              |
| reset               | Displays the number times a CPE has been reset                                                                                                                                                                                                       |
| system              | Displays device hardware and SKU information for each CPE. Use this information to assess whether a controller is managing the correct CPE devices out of the total number of CPEs available.                                                        |
| uptime              | Displays the time each CPE device has been actively deployed and operational                                                                                                                                                                         |
| version             | Displays the application and boot versions utilized by the CPE devices                                                                                                                                                                               |
| on <T5-DEVICE-NAME> | Optional. Executes the command on a specified T5 device <ul style="list-style-type: none"> <li>• &lt;T5-DEVICE-NAME&gt; - Specify the T5 device's hostname. An error message is displayed if no T5 device name is specified.</li> </ul>              |

```
show t5 interface [dsl|fe|ge] [counter|description|errors|status|utilization]
{on <T5-DEVICE-NAME>}
```

|           |                                                                          |
|-----------|--------------------------------------------------------------------------|
| t5        | Displays adopted T5 controller statistics                                |
| interface | Displays T5 interface-related statistics based on the interface selected |

[dsl|fe|ge|radio] [counter|description| errors|status|utilization]

Select the interface type. The options are: dsl, fe, ge.

- dsl – Displays DSL (Digital Subscriber Line) interface related information
- fe – Displays FE (Fast Ethernet) interface related information
- ge – Displays GE (Gigabit Ethernet) interface related information

The system displays the following information for the DSL, GE, and FE ports:

- counter – Displays the following:
  - Number of octets (bytes) received and transmitted on this port
  - Number of data packets received and transmitted on this port
  - Number of flow control (layer 2) packets received and transmitted on this port
- description – Displays the following:
  - The selected port's name
  - The numeric index assignable to each port
  - The 64 character maximum, unique, administrator-assigned description to each port
- errors – Displays the following DSL interface related errors:
  - The name of the DSL utilized by each T5 controller connected CPE device
  - The number of FECs detected in the downstream direction. FEC (Forward Error Correction) or channel coding is used for controlling errors over unreliable or noisy communication channels.
  - The number of CPE DSL coding violations (badly coded packets) detected in the downstream direction.
  - The number of FECs detected in the upstream direction.
  - The number of CPE DSL coding violations (badly coded packets) detected in the upstream direction.
- status – Displays the following:
  - The selected port's name
  - Whether the port is currently up or down as a T5 controller transmit and receive resource
  - The port's current speed in MB
  - Whether pause packet utilization is currently off or on for the selected port
  - Whether each listed port is enabled or disabled by the administrator
- utilization – Displays the following:
  - The selected port's name
  - The port's receive and transmit data rates (in Kbps)
  - The packet per second port receive and transmit rates (p/s)
  - Each port's receive and transmit direction utilization as a percentage of the total transmit bandwidth available.

on <T5-DEVICE-NAME>

Optional. Executes the command on a specified T5 device

- <T5-DEVICE-NAME> – Specify the T5 device's hostname. An error message is displayed if no T5 device name is specified.

```
show t5 interface dsl custom [avg|dses|dsses|peak|uses|usses]
{on <T5-DEVICE-NAME>}
```

|           |                                                                          |
|-----------|--------------------------------------------------------------------------|
| t5        | Displays adopted T5 controller statistics                                |
| interface | Displays T5 interface-related statistics based on the interface selected |

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dsl                                     | <p>Selects A T5 controller's DSL interface.</p> <p>A T5 controller uses the operating system to manage its connected radio devices, as opposed to the WiNG operating used by RFS controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The CPEs are the T5 controller managed radio devices using the operating system. These CPEs use a DSL as their high speed Internet access mechanism using the CPE's physical wallplate connection and phone jack.</p>                                                                                                                      |
| custom [avg dses dsses peak uses usses] | <p>Displays following custom CPE DSL data:</p> <ul style="list-style-type: none"> <li>• avg - Each DSL's average response time in microseconds</li> <li>• dses - The number of seconds downstream DSL transmissions were negatively impacted by code violations.</li> <li>• dsses - The number of seconds downstream DSL transmissions were severely negatively impacted by code violations.</li> <li>• peak - Each DSL's maximum (best to date since the screen was refreshed) response time in microseconds.</li> <li>• uses - The number of seconds upstream DSL transmissions were negatively impacted by code violations.</li> <li>• usses - The number of seconds upstream DLS transmissions were severely negatively impacted by code violations.</li> </ul> |
| on <T5-DEVICE-NAME>                     | <p>Optional. Executes the command on a specified T5 device</p> <ul style="list-style-type: none"> <li>• &lt;T5-DEVICE-NAME&gt; - Specify the T5 device's hostname. An error message is displayed if no T5 device name is specified.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

```
show t5 interface radio [stats|status|wlam-map] {on <T5-DEVICE-NAME>}
```

|           |                                                                          |
|-----------|--------------------------------------------------------------------------|
| t5        | Displays adopted T5 controller statistics                                |
| interface | Displays T5 interface-related statistics based on the interface selected |

radio [stats|status| wlan-map]

Displays following radio interface related information:

- stats – Displays T5 radio interface statistics. A T5 controller uses the operating system to manage its connected radio devices, as opposed to the WiNG operating used by RFS controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The CPEs are the T5 controller managed radio devices using the operating system. Use this option to view the following:
  - name – The administrator assigned name of each listed CPE radio as its unique identifier
  - Rx (Kbps) – The listed CPE radio's receive data rate (in Kbps). Use this information to assess RF activity versus other T5 managed CPE radios in the same radio coverage area.
  - Rx Octets – The number of octets (bytes) received with no errors by the listed T5 controller managed CPE radio.
  - Rx Packets – The number of data packets received for the listed T5 managed CPE radio since this screen was last refreshed.
  - Tx (Kbps) – The listed CPE radio's transmit data rate (in Kbps). Use this information to assess RF activity versus other T5 managed CPE radios in the same radio coverage area.
  - Tx Octets – Displays the number of octets (bytes) transmitted with no errors by the listed T5 controller managed CPE radio.
  - Tx Packets – The number of data packets transmitted from the listed T5 managed CPE radio since this screen was last refreshed.
- status – Displays T5 radio interface status information
  - name – The administrator assigned name of each listed CPE radio as its unique identifier.
  - Operational status – The radio interface's operational status (enabled/disabled).
  - mac – The T5 radio interface's MAC address.
  - transmit power – The T5 radio interface's transmit power.
  - Channel – The T5 radio interface's channel of operation.
- wlan-map – Displays WLAN map membership data for T5 controller managed CPE radio devices. Use this option to view the following:
  - name – The administrator assigned name of each listed CPE radio as its unique identifier.
  - status – Whether a CPE radio is currently enabled or disabled as a radio resource for the WLAN(s) the CPE radio has been mapped to.
  - wlan-radio-mapping – The managed WLAN(s) each listed radio has been mapped to.

on <T5-DEVICE-NAME>

Optional. Executes the command on a specified T5 device

- <T5-DEVICE-NAME> – Specify the T5 device's hostname. An error message is displayed if no T5 device name is specified.

```
show t5 mac table [filter name [dsl<1-24>|ge <1-2>|vlan <1-4094>|wlan <1-24>]
{on <T5-DEVICE-NAME>}
```

|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| t5                                                         | Displays adopted T5 controller statistics                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| mac table [dsl<1-24> ge <1-2>  vlan <1-4094>  wlan <1-24>] | <p>Displays T5 MAC address table. The T5 MAC table displays a dynamic list of MAC addresses learned by the T5 controller over its ethernet interfaces. Use this information to identify devices and the interfaces on which they can be found.</p> <p>Use the following additional filters to filter on the basis of the VLAN or DSL interface:</p> <ul style="list-style-type: none"> <li>• dsl &lt;1-24&gt; - Filters information on the basis of the selected DSL port</li> <li>• ge &lt;1-2&gt; - Filters information on the basis of the selected GE port</li> <li>• vlan &lt;1-4094&gt; - Filters information on the basis of the selected VLAN port</li> <li>• wlan &lt;1-24&gt; - Filters on the basis of the selected CPE</li> </ul> |
| on <T5-DEVICE-NAME>                                        | <p>Optional. Executes the command on a specified T5 device</p> <ul style="list-style-type: none"> <li>• &lt;T5-DEVICE-NAME&gt; - Specify the T5 device's hostname. An error message is displayed if no T5 device name is specified.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

```
show t5 wireless client {filter name [association-status/authentication-status/bss/mac-address/retry-percentage/rssi-value]} {on <T5-DEVICE-NAME>}
```

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| t5                  | Displays adopted T5 controller statistics                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| wireless client     | <p>Displays the T5 wireless client and WLAN related statistics</p> <ul style="list-style-type: none"> <li>• client - Displays read-only device information for wireless clients associated with the selected T5 controller and its connected CPE device radios. Use this information to assess if configuration changes are required to improve client performance.</li> </ul> <p>Use the additional filters available to view specific client-related information. The options are:</p> <ul style="list-style-type: none"> <li>• association-status</li> <li>• authentication-status</li> <li>• bss</li> <li>• retry-percentage</li> <li>• rssi-value</li> </ul> |
| on <T5-DEVICE-NAME> | <p>Optional. Executes the command on a specified T5 device</p> <ul style="list-style-type: none"> <li>• &lt;T5-DEVICE-NAME&gt; - Specify the T5 device's hostname. An error message is displayed if no T5 device name is specified.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                    |

```
show t5 wireless wlan counters [qos|rate|size] {on <T5-DEVICE-NAME>}
```

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| t5                            | Displays adopted T5 controller statistics                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| wireless wlan [qos rate size] | <p>Displays the T5 wireless WLAN related statistics</p> <ul style="list-style-type: none"> <li>wlan – Displays following T5 controller traffic counter statistics: <ul style="list-style-type: none"> <li>qos – T5 controller WLAN QoS utilization. Displays the number of background (low priority) and best-effort packets received and transmitted on each listed T5 controller managed WLANs</li> <li>rates – Displays T5 controller's WLAN utilization data rate statistics <ul style="list-style-type: none"> <li>Lists the number of data packets received and transmitted in the WLAN that have been relegated to a 1 Mbps data rate</li> <li>Lists the number of data packets received and transmitted in the WLAN by T5 controller connected devices at 54Mbps</li> </ul> </li> <li>size – Displays the number of data packets received and transmitted, in each listed WLAN, greater than 1024 bytes</li> </ul> </li> </ul> |
| on <T5-DEVICE-NAME>           | <p>Optional. Executes the command on a specified T5 device</p> <ul style="list-style-type: none"> <li>&lt;T5-DEVICE-NAME&gt; – Specify the T5 device's hostname. An error message is displayed if no T5 device name is specified.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Examples

The following examples are for show commands executed on the 't5-ED7C6C' controller adopted by the 'nx9500-6C8809' wireless controller:

```

nx9500-6C8809(config)#show t5 boot on t5-ED7C6C
Primary Version: 5.4.2.0-010R
Secondary Version: 5.4.2.0-006B
Next Boot: Primary
Upgrade Status: none
Upgrade Progress %: 0
nx9500-6C8809(config)#
nx9500-6C8809(config)#show t5 version on t5-ED7C6C
Bootloader Version: 5.4.2.0-010R
Application Version: 5.4.2.0-010R
nx9500-6C8809(config)#
nx9500-6C8809(config)#show t5 system on t5-ED7C6C
Serial Number 14213522400004
SKU TS-0524-WR
Hardware Rev 5
Mac Address B4-C7-99-ED-7C-6C
Description 24-port PowerBroadband VDSL2 Switch Version 5.4.2.0-010R
Contact NULL
Name t5-ED7C6C
Location NULL
nx9500-6C8809(config)#
nx9500-6C8809(config)#show t5 clock on t5-ED7C6C
Time 6-6-2017 17:14:30 UTC
nx9500-6C8809(config)#
nx9500-6C8809(config)#show t5 interface ge counter on t5-ED7C6C

INTERFACE RECEIVE OCTETS RECEIVE PACKETS RECEIVE PAUSE PKTS TRANSMIT OCTETS TRANSMIT
PACKETS TRANSMIT PAUSE PKTS

ge1 711128918 89636040 0 2558110037
133720283 0
ge2 2515775064 133311355 0 3422167586
78735853 0

```



```

nx9500-6C8809(config)#
nx9500-6C8809(config)#show t5 uptime on t5-ED7C6C
Up Time 0 days 1 day, 3:19:43
nx9500-6C8809(config)#
nx9500-6C8809(config)#show t5 temperature on t5-ED7C6C
===== Temperature =====

INDEX CURRENT (C) FANS @ FULL SPEED (C) FANS @ VARIABLE SPEED (C)

1 39 70 60

```

```

nx9500-6C8809(config)#
nx9500-6C8809(config)#show t5 cpe address on t5-ED7C6C

DEVICE STATUS IP ADDRESS MAC ADDRESS

cpe1 ready 192.168.13.32 00-C0-23-69-80-CD
cpe2 ready 192.168.13.33 74-6F-F7-40-16-62
cpe3 disconnected 0.0.0.0 00-00-00-00-00-00
cpe4 disconnected 0.0.0.0 00-00-00-00-00-00
cpe5 disconnected 0.0.0.0 00-00-00-00-00-00

```

```

--More--
nx9500-6C8809(config)#
nx9500-6C8809(config)#show t5 cpe led on t5-ED7C6C

DEVICE LED STATUS

cpe1 enable
cpe2 enable
cpe3 enable
cpe4 enable
cpe5 enable

```

```

--More--
nx9500-6C8809(config)#
nx9500-6C8809(config)#show t5 mac table filter name vlan 1 on t5-ED7C6C

T5-MAC VLAN ADDRESS INTERFACE VENDOR

B4-C7-99-ED-7C-6C 1 00-02-B3-28-D1-55 ge1 Intel Corp
B4-C7-99-ED-7C-6C 1 00-1E-67-4B-BF-BD ge1 Intel Corp
B4-C7-99-ED-7C-6C 1 00-23-68-11-E6-C4 ge1 Extreme
Tech
B4-C7-99-ED-7C-6C 1 00-23-68-88-0D-A7 ge1 Extreme
Tech
B4-C7-99-ED-7C-6C 1 00-23-68-99-BB-7C ge1 Extreme
Tech
B4-C7-99-ED-7C-6C 1 00-A0-F8-68-D5-70 ge1 Extreme
Tech
B4-C7-99-ED-7C-6C 1 00-C0-23-69-80-CD ds11 00-C0-23
B4-C7-99-ED-7C-6C 1 1C-7E-E5-18-FA-67 ge1 D-Link
Corp
B4-C7-99-ED-7C-6C 1 3C-CE-73-F4-47-83 ge1 Cisco
Systems
B4-C7-99-ED-7C-6C 1 74-6F-F7-40-16-62 ds12 Wistron
Corp
--More--
nx9500-6C8809(config)#

```



---

## *terminal*

Displays terminal configuration parameters

### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### **Syntax**

```
show terminal
```

### **Parameters**

None

### **Examples**

```
nx9500-6C8809(config)#show terminal
Terminal Type: xterm
Length: 24 Width: 200
nx9500-6C8809(config)#
```

## *timezone*

Displays a device's timezone

### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### **Syntax**

```
show timezone
```

### **Parameters**

None

### **Examples**

```
nx9500-6C8809(config)#show timezone
Timezone is America/Los_Angeles
nx9500-6C8809(config)#
```

## *traffic-shape*

Displays traffic-shaping related configuration details and statistics

Traffic shaping regulates network data transfers to ensure a specific performance level. Traffic shaping delays the flow of packets defined as less important than prioritized traffic streams. Traffic shaping enables traffic control out an interface to match its flow to the speed of a remote target's interface and ensure traffic conforms applied policies. Traffic can be shaped to meet downstream requirements and eliminate network congestion when data rates are in conflict.

Apply traffic shaping to specific applications to apply application categories. When application and ACL rules are conflicting, ACL rules take precedence for the traffic shaping class. Using traffic shaping, an application takes precedence over an application category.

**Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

**Syntax**

```
show traffic-shape [priority-map|statistics {class <1-4>}|status] {on <DEVICE-NAME>}
```

**Parameters**

```
show traffic-shape [priority-map|statistics {class <1-4>}|status] {on <DEVICE-NAME>}
```

|                        |                                                                                                                                                                                                                                                                                                                                                           |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| traffic-shape          | Displays traffic-shaping related configuration details and statistics                                                                                                                                                                                                                                                                                     |
| priority-map           | Displays the traffic shaper queue priority. There are 8 queues (0 - 7), and traffic is queued in each based on incoming packets 802.1p markings.                                                                                                                                                                                                          |
| statistics class <1-4> | Displays traffic-shaping related statistics for all traffic shaper classes or for a selected class <ul style="list-style-type: none"> <li>• class &lt;1-4&gt; - Optional. Specify the traffic class from 1 - 4. The system displays traffic shaping statistics for the selected class. If not selected, the system statistics for all classes.</li> </ul> |
| status                 | Displays the controller or service platform's traffic shaping status (whether running or not)                                                                                                                                                                                                                                                             |
| on <DEVICE-NAME>       | Optional. Displays traffic-shaping related configuration details and statistics on a specified device <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li> </ul>                                                                                                     |

**Examples**

```
ap7532-DEB9B0#show traffic-shape priority-map
```

```

 DOT1P-PRIORITY TX-SHAPER-PRIORITY

 0 2
 1 0
 2 1
 3 3
 4 4
 5 5
 6 6
 7 7

```

```
ap7532-DEB9B0#
ap7532-DEB9B0#show traffic-shape status
State of Traffic shaper: running
ap7532-DEB9B0#
ap7532-DEB9B0#show traffic-shape statistics
```

```
Traffic shaper class : 1
Class 1 is not configured:
```



Traffic shaper class : 3  
Class 3 is not configured:

Traffic shaper class : 2  
Rate: 1500 Kbps

| PRIORITY | PKTS-SENT | PKTS-DELAYED | PKTS-DROPPED | CURRENT-QUEUE-LEN | CURRENT-LATENCY (IN USECS) |
|----------|-----------|--------------|--------------|-------------------|----------------------------|
| 1        | 0         | 0            | 0            | 0                 | 0                          |
| 0        | 0         | 0            | 0            | 0                 | 0                          |
| 3        | 0         | 0            | 0            | 0                 | 0                          |
| 2        | 152153035 | 151924251    | 1508343      | 11                | 33447                      |
| 5        | 0         | 0            | 0            | 0                 | 0                          |
| 4        | 0         | 0            | 0            | 0                 | 0                          |
| 7        | 0         | 0            | 0            | 0                 | 0                          |
| 6        | 0         | 0            | 0            | 0                 | 0                          |

Traffic shaper class : 4  
Class 4 is not configured:  
ap7532-DEB9B0#

### upgrade-status

Displays the last image upgrade status



#### Note

This command is not available in the USER EXEC Mode.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show upgrade-status {detail/on}
show upgrade-status {detail} {(on <DEVICE-NAME>)}
```

### Parameters

```
show upgrade-status {detail} {(on <DEVICE-NAME>)}
```

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| upgrade-status   | Displays last image upgrade status and log                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| detail           | Optional. Displays last image upgrade status in detail                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| on <DEVICE-NAME> | The following keyword is recursive and common to the 'detail' parameter: <ul style="list-style-type: none"><li>• on &lt;DEVICE-NAME&gt; - Optional. Displays last image upgrade status on a specified device</li><li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li></ul> <p><b>Note:</b> If the 'on' keyword is used without the 'detail' keyword, the system displays a summary of upgrade status and log on the specified device.</p> |

## Examples

```
nx9500-6C8809#show upgrade-status
Last Image Upgrade Status :In_Progress(17 percent completed)
Last Image Upgrade Time : 2017-02-11 12:26:29
nx9500-6C8809#
nx9500-6C8809#show upgrade-status detail
Last Image Upgrade Status : Successful
Last Image Upgrade Time : 2017-06-02 14:22:51

Running from partition /dev/sda8
var2 is 1 percent full
/tmp is 4 percent full
Free Memory 33357504 kB
FWU invoked via Linux shell
Validating image file header
Removing other partition
Tue May 30 10:43:36 IST 2017
debug: cmdline -C /boot/lilo.conf -R 5.9.0.0-028B -P fix
LILO version 22.6-CCB, Copyright (C) 1992-1998 Werner Almesberger
--More--
nx9500-6C8809#
```

## version

Displays a device's software and hardware version

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show version {on <DEVICE-NAME>}
```

### Parameters

```
show version {on <DEVICE-NAME>}
```

|                            |                                                                                              |
|----------------------------|----------------------------------------------------------------------------------------------|
| version {on <DEVICE-NAME>} | Displays software and hardware versions on all devices or a specified device                 |
|                            | • on <DEVICE-NAME> - Optional. Displays software and hardware versions on a specified device |
|                            | • <DEVICE-NAME> - Specify the name of the AP, wireless controller, or service platform.      |

## Examples

```
nx9500-6C8809#show version
NX9500 version 5.9.2.0-008D
Copyright (c) 2004-2018 Extreme Networks, Inc. All rights reserved.
Booted from secondary

NOC-NX9500 uptime is 10 days, 01 hours 34 minutes
CPU is Intel(R) Xeon(R) CPU E5645 @ 2.40GHz, No. of CPUs 24
Base ethernet MAC address is B4-C7-99-6C-88-09
System serial number is B4C7996C8809
Model number is NX-9500-100R0-WR

nx9500-6C8809#
```

## vrrp

Displays VRRP (Virtual Router Redundancy Protocol) protocol details

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show vrrp [brief|details|error-stats|stats]
show vrrp [brief|details|stats] {<1-255>} {(on <DEVICE-NAME>)}
show vrrp error-stats {on <DEVICE-NAME>}
```

### Parameters

```
show vrrp [brief|details|stats] {<1-255>} {(on <DEVICE-NAME>)}
```

|                  |                                                                                                                                                                                                                                                                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vrrp             | Displays VRRP related statistics in brief or in detail depending on the option selected                                                                                                                                                                                                                                          |
| brief            | Displays virtual router information in brief                                                                                                                                                                                                                                                                                     |
| details          | Displays virtual router information in detail                                                                                                                                                                                                                                                                                    |
| stats            | Displays virtual router statistics                                                                                                                                                                                                                                                                                               |
| <1-255>          | The following keyword is common to all of the above parameters: <ul style="list-style-type: none"><li>• &lt;1-255&gt; – Optional. Displays information for a specified Virtual Router. Specify the router's ID from 1 -255.</li></ul>                                                                                            |
| on <DEVICE-NAME> | The following keyword is recursive and common to the '<1-255>' parameter: <ul style="list-style-type: none"><li>• on &lt;DEVICE-NAME&gt; – Optional. Displays specified router information on a specified device</li><li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li></ul> |

```
show vrrp error-stats {on <DEVICE-NAME>}
```

|                                |                                                                                                                                                                                                                                                                                    |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vrrp                           | Displays VRRP related statistics in brief or in detail depending on the option selected                                                                                                                                                                                            |
| error-stats {on <DEVICE-NAME>} | Displays global error statistics <ul style="list-style-type: none"><li>• on &lt;DEVICE-NAME&gt; – Optional. Displays global error statistics on a specified device</li><li>• &lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li></ul> |

### Examples

```
nx9500-6C8809(config)#show vrrp error-stats
Last protocol error reason: none
IP TTL errors: 0
Version mismatch: 0
Packet Length error: 0
Checksum error: 0
Invalid virtual router id: 0
Authentication mismatch: 0
```

```

Invalid packet type: 0
nx9500-6C8809(config)#
nx9500-6C8809(config)#show vrrp details
VRRP Group 1:
 version 2
 interface none
 configured priority 1
 advertisement interval 1 sec
 preempt enable, preempt-delay 0
 virtual mac address 00-00-5E-00-01-01
 sync group disable
nx9500-6C8809(config)#

```

## virtual-machine

Displays the VM (virtual-machine) configuration, logs, and statistics

### Supported in the following platforms:

- Service Platforms — NX 7510, NX 95XX

### Syntax

```

show virtual-machine [configuration|debugging|export|statistics]
show virtual-machine [configuration|statistics] {<VM-NAME>/team-urc/team-rls/
team-vowlan} {(on <DEVICE-NAME>)}
show virtual-machine debugging {level/on}
show virtual-machine debugging {level [debug/error/info/warning]} {on <DEVICE-NAME>}
show virtual-machine export <VM-NAME> {on <DEVICE-NAME>}
show virtual-machine [configuration|statistics] {<VM-NAME>/adsp/team-cmt}

```

### Parameters

```

show virtual-machine [configuration|statistics] {<VM-NAME>/team-urc/team-rls/
team-vowlan} {(on <DEVICE-NAME>)}

```

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| virtual-machine                             | Displays the following VM-related information: configuration or statistics                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| configuration                               | Displays detailed VM configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| statistics                                  | Displays VM statistics                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| [<VM-NAME>] team-urc team-rls  team-vowlan] | The following keywords are common to the 'configuration' and 'statistics' parameters: <ul style="list-style-type: none"> <li>• VM-NAME&gt; - Optional. Displays VM configuration or statistics for the virtual machine identified by the &lt;VM-NAME&gt; keyword. Specify the VM name.</li> <li>• team-urc - Optional. Displays TEAM-URC (IP-PBX) VM configuration/statistics</li> <li>• team-rls - Optional. Displays TEAM-RLS (Radio Link Server) VM configuration/statistics&lt;</li> <li>• team-vowlan - Optional. Displays TEAM-VoWLAN (Voice over WLAN) VM configuration/statistics</li> </ul> |
| on <DEVICE-NAME>                            | Specifies the name of the device on which the command is executed <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the service platform.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                |

```

show virtual-machine [configuration|statistics] {<VM-NAME>/adsp/team-cmt} {(on <DEVICE-
NAME>)}

```

|                 |                                                                            |
|-----------------|----------------------------------------------------------------------------|
| virtual-machine | Displays the following VM-related information: configuration or statistics |
| configuration   | Displays detailed VM configuration                                         |

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| statistics                    | Displays VM statistics                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| [<VM-NAME> adsp <br>team-cmt] | The following keywords are common to the 'configuration' and 'statistics' parameters: <ul style="list-style-type: none"> <li>• VM-NAME&gt; – Optional. Displays VM configuration or statistics for the virtual machine identified by the &lt;VM-NAME&gt; keyword. Specify the VM name.</li> <li>• adsp – Optional. Displays ADSP (Air-Defense Services Platform) VM configuration/statistics</li> <li>• team-cmt – Optional. Displays TEAM-CMT VM configuration/statistics</li> </ul> |
| on <DEVICE-NAME>              | Specifies the name of the device on which the command is executed<br><DEVICE-NAME> – Specify the name of the service platform.                                                                                                                                                                                                                                                                                                                                                        |

```
show virtual-machine debugging {level[debug/error/info/warning]} {on <DEVICE-NAME>}
```

|                                       |                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| virtual-machine                       | Displays the following VM-related information: configuration or statistics                                                                                                                                                                                                                                                                                                     |
| debugging                             | Displays VM debugging logs                                                                                                                                                                                                                                                                                                                                                     |
| level [debug  error <br>info warning] | Optional. Displays VM debugging logs based on the level selected. The available options are: <ul style="list-style-type: none"> <li>• debug – Displays VM logs of level debug and above</li> <li>• error – Displays VM logs of level error</li> <li>• info – Displays VM logs of level Info and above</li> <li>• warning – Displays logs of level warning and above</li> </ul> |
| on <DEVICE-NAME>                      | Specifies the name of the device on which the command is executed <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the service platform.</li> </ul>                                                                                                                                                                                          |

```
show virtual-machine export <VM-NAME> {on <DEVICE-NAME>}
```

|                      |                                                                                                                                                                                                                                                                |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| virtual-machine      | Displays the following VM-related information: configuration or statistics                                                                                                                                                                                     |
| export               | Displays VM configuration export related information                                                                                                                                                                                                           |
| <VM-NAME>]           | Displays VM configuration export related information for the virtual machine identified by the <VM-NAME> keyword. Specify the VM name.<br>The NX 9500 and NX 9510 series service platforms will display ADSP and TEAM-CMT VM configuration export information. |
| on <DEVICE-<br>NAME> | Specifies the name of the device on which the command is executed <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Specify the name of the service platform.</li> </ul>                                                                          |

## Examples

```
nx9500-6C8809#show virtual-machine statistics
```

```

```

| NAME     | STATE  | VCPUS | MEM (MB) | BRIDGE-IF | IP |
|----------|--------|-------|----------|-----------|----|
| WiNG     | -      | -     | 18432    | -         | -  |
| adsp     | Halted | -     | -        | unknown   | -  |
| team-cmt | Halted | -     | -        | unknown   | -  |

```

```

```
nx9500-6C8809#
```

```
nx9500-6C8809#show virtual-machine configuration
```

```

```

| NAME | AUTOSTART | MEMORY (MB) | VCPUS |
|------|-----------|-------------|-------|
| WiNG | -         | 18432       | -     |
| adsp | ignore    | 12000       | 12    |

```

```



```

team-cmt ignore 1024 1

nx9500-6C8809#
nx9500-6C8809>show virtual-machine statistics adsp
 VM name: adsp
 Base Version : unknown
 Install Status : not_installed
nx9500-6C8809>

```

### web-filter

Displays Web filtering related information

Use this command to view information on Web requests for content and whether the requests were blocked or approved based on URL filter settings defined for the selected controller or service platform. A URL filter is comprised of several filter rules. A whitelist bans all sites except the categories and URL lists defined in the whitelist. The blacklist allows all sites except the categories and URL lists defined in the blacklist.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562
- Wireless Controllers — RFS 4000
- Service Platforms — NX 7510, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
show web-filter [category|category-type|config|filter-level [basic|high|low|medium|medium-high]|statistics {on <DEVICE-NAME>}|status]
```

#### Parameters

```
show web-filter [category|category-type|config|filter-level [basic|high|low|medium|medium-high]|statistics {on <DEVICE-NAME>}|status]
```

|                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| web-filter                                         | Displays an existing and configured Web filter details                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| category                                           | Displays Web filter categories. A category is a pre-defined URL list available in the WING software.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| category-type                                      | Displays the Web filter category types. This is a pre-configured list of categories and sub-categories in to which commonly accessed URLs have been classified.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| config                                             | Displays all existing Web filters and their configuration details                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| filter-level [basic  high low medium  medium-high] | Displays category types for the selected filter-level. Each filter level is pre-configured to use a set of category types. You cannot change the categories in the category types used for these pre-configured filter-level setting. Nor can you add, modify, or remove the category types mapped to a filter-level setting. The options are: <ul style="list-style-type: none"> <li>• basic - Displays all category types configured for the basic filter-level</li> <li>• high - Displays all category types configured for the high filter-level</li> <li>• low - Displays all category types configured for the low filter-level</li> <li>• medium - Displays all category types configured for the medium filter-level</li> <li>• medium-high - Displays all category types configured for the medium-high filter-level</li> </ul> |

|                                                |                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>statistics {on &lt;DEVICE-NAME&gt;}</pre> | <p>Displays Web filter statistics on a specified device</p> <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; – Optional. Specifies the device name</li> <li>&lt;DEVICE-NAME&gt; – Specify the name of the AP, controller, or service platform.</li> </ul> <p><b>Note:</b> Web filtering is a licensed feature, and only when enforced can the system display Web filtering statistics.</p> |
| <pre>status {on &lt;DEVICE-NAME&gt;}</pre>     | <p>Displays Web filter status on a specified device</p> <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; – Optional. Specifies the device name</li> <li>&lt;DEVICE-NAME&gt; – Specify the name of the AP, controller, or service platform.</li> </ul> <p><b>Note:</b> Web filtering is a licensed feature, and only when enforced can the system display Web filtering status.</p>         |

## Examples

```

nx9500-6C8809(config)#show web-filter category
 advertisement-popups
 Sites that provide advertising graphics or other ad content
 files such as banners and pop-ups.
 alcohol-tobacco
 Sites that promote or sell alcohol- or tobacco-related
 products or services.
 anonymizers
 Sites and proxies that act as an intermediary for surfing to
 other websites in an anonymous fashion, whether to
 circumvent web filtering or for other reasons.
 arts
 Sites with artistic content or relating to artistic
 institutions such as theaters, museums, galleries, dance
 companies, photography, and digital graphic resources.
 botnets
 Sites that use bots (zombies) including command-and-control
 sites.
--More--
nx9500-6C8809(config)#
nx9500-6C8809(config)#show web-filter config
URL filters configured for this device are:
 WebFilter_ShoppingSites
 Blacklisted categories:
 shopping,
 Whitelisted categories:
 <AllowedShopping>,
nx9500-6C8809(config)#

```

*what*

Displays details of a specified search phrase (performs global search)

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
show what [contain|is] <WORD> {on <DEVICE-OR-DOMAIN-NAME>}
```

## Parameters

```
show what [contain|is] <WORD> {on <DEVICE-OR-DOMAIN-NAME>}
```

|                            |                                                                                                                                                                                                                                      |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| contain <WORD>             | Searches for all items that contain a specified word <ul style="list-style-type: none"><li>&lt;WORD&gt; - Specify the string to use as match criteria (for example, MAC address, hostname, etc.).</li></ul>                          |
| is <WORD>                  | Searches for items exactly matching a specified string <ul style="list-style-type: none"><li>Specify the string to use as match criteria (for example, MAC address, hostname, etc.).</li></ul>                                       |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Performs global search on a specified device or RF Domain <ul style="list-style-type: none"><li>&lt;DEVICE-OR-DOMAIN-NAME&gt; - Specify the name of the AP, wireless controller, service platform, or RF Domain.</li></ul> |

## Examples

```
rfs4000-229D58#show what contain default
```

```

NO. CATEGORY MATCHED OTHER KEY INFO (1)
OTHER KEY INFO (2) OTHER KEY INFO (3)
NAME/VALUE NAME/VALUE NAME/VALUE

mac https-trustpoint type
 rf_domain_name
1 device-cfg fault-finders rfs4000
00-23-68-22-9D-58 default

 __obj_name__
name
2 firewall_policy
default

 __obj_name__ name
HTTPS idle_session_timeout
3 management_policy default
True 30

control_vlan qos_policy name
 beacon_format

--More--
rfs4000-229D58#
```

## wireless

Displays wireless configuration information and statistics

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533

- 
- Wireless Controllers — RFS 4000
  - Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
show wireless [ap|bridge|client|coverage-hole-incidents|meshpoint|mint|mobility-database|
radio|regulatory|rf-domain|sensor-server|unsanctioned|wips|wlan]
show wireless ap {configured/detail/load-balancing/on <DEVICE-NAME>}
show wireless ap {configured}
show wireless ap {detail} {<MAC/HOST-NAME>} {(on <DEVICE-OR-DOMAIN-NAME>)}
show wireless ap {load-balancing} {client-capability/events/neighbors} {(on <DEVICE-
NAME>)}
show wireless bridge {candidate-ap/certificate/config/hosts/on/statistics}
show wireless bridge {candidate-ap} {<MAC/HOSTNAME> {<1-3>}} {(filter radio-mac
<RADIO-MAC>)} {(on <DEVICE-OR-DOMAIN-NAME>)}
show wireless bridge {certificate} status {on <DEVICE-NAME>}
show wireless bridge {config}
show wireless bridge {hosts} {on <DEVICE-OR-DOMAIN-NAME>}
show wireless bridge {statistics} {rf/traffic} {(on <DEVICE-OR-DOMAIN-NAME>)}
show wireless client {association-history/detail/filter/include-ipv6/on <DEVICE-OR-DOMAIN-
NAME>|
statistics/tspec}
show wireless client {association-history <MAC>} {on <DEVICE-OR-DOMAIN-NAME>}

show wireless client {detail <MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}
show wireless client {filter [ip/on/state/wlan]}
show wireless client {filter} {ip [<IP>/not <IP>]} {on <DEVICE-OR-DOMAIN-NAME>}
show wireless client {filter} {on <DEVICE-OR-DOMAIN-NAME>}
show wireless client {filter} {state data-ready/not [data-ready/roaming]|
roaming]} {on <DEVICE-OR-DOMAIN-NAME>}
show wireless client {filter} {wlan [<WLAN-NAME>|not <WLAN-NAME>]}
{on <DEVICE-OR-DOMAIN-NAME>}
show wireless client {include-ipv6} {detail/on/filter}
show wireless client {include-ipv6} {detail <MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}
show wireless client {include-ipv6} {filter {ip/ipv6/state/wlan}}
show wireless client {statistics} {detail/on/rf/window-data}
show wireless client {statistics} {detail <MAC>|rf/window-data <MAC>}
{(on <DEVICE-OR-DOMAIN-NAME>)}
show wireless client {tspec <MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}
show wireless coverage-hole-incidents [detail/on/summary]
show wireless coverage-hole-incidents detail {filter [ap <MAC/HOSTNAME>|client-mac <MAC>]|
summary} {(on <DOMAIN-NAME>)}
show wireless meshpoint {config/detail/multicast/neighbor/on/path/proxy/root/security|
statistics/tree/usage-mappings}
show wireless meshpoint {config} {filter [device <DEVICE-NAME>|rf-domain <DOMAIN-NAME>]}
show wireless meshpoint {detail} {<MESHPOINT-NAME>}
show wireless meshpoint {on <DEVICE-OR-DOMAIN-NAME>}
show wireless meshpoint {multicast/path/proxy/root/security/statistics} [<MESHPOINT-NAME>|
detail]
{on <DEVICE-OR-DOMAIN-NAME>}
show wireless meshpoint neighbor [<MESHPOINT-NAME>|detail/statistics {rf}]
{on <DEVICE-OR-DOMAIN-NAME>}
show wireless meshpoint {tree} {on <DEVICE-OR-DOMAIN-NAME>}
show wireless meshpoint {usage-mappings}
show wireless mobility-database {on <DEVICE-NAME>}
show wireless mint [client/detail/links/portal]
show wireless [client/detail] {on/portal-candidates {<DEVICE-NAME>|
filter <RADIO-MAC>}/statistics} (<DEVICE-OR-DOMAIN-NAME>)
show wireless mint links {on <DEVICE-OR-DOMAIN-NAME>}
show wireless mint portal statistics {on <DEVICE-OR-DOMAIN-NAME>}
show wireless radio {detail/on <DEVICE-OR-DOMAIN-NAME>|statistics/tspec/wlan-map}
show wireless radio {detail} {<DEVICE-NAME>|filter/on <DEVICE-OR-DOMAIN-NAME>}
show wireless radio {detail} {<DEVICE-NAME> {<1-3>|filter/on}}
show wireless radio {detail} {filter <RADIO-MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}
show wireless radio {statistics} {detail/on/rf/windows-data}
show wireless radio {statistics} {on <DEVICE-OR-DOMAIN-NAME>|
rf {on <DEVICE-OR-DOMAIN-NAME>}}
show wireless radio {statistics} {detail/window-data} {<DEVICE-NAME>} {<1-3>|
filter <RADIO-MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}
show wireless radio {tspec} {<DEVICE-NAME>|filter/on <DEVICE-OR-DOMAIN-NAME>|option}
show wireless radio {wlan-map} {on <DEVICE-OR-DOMAIN-NAME>}
show wireless regulatory [channel-info <WORD>|country-code <WORD>|device-type]
show wireless regulatory device-type [ap6522|ap6562|ap7161|ap7502|ap7522|ap7532|
```

```

ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap8163|ap8432|ap8533] <WORD>
show wireless rf-domain statistics {detail} {(on <DEVICE-OR-DOMAIN-NAME>)}
show wireless sensor-server {on <DEVICE-OR-DOMAIN-NAME>}
show wireless unsanctioned aps {detail/statistics} {(on <DEVICE-OR-DOMAIN-NAME>)}
show wireless wips [client-blacklist|event-history] {on <DEVICE-OR-DOMAIN-NAME>}
show wireless wlan {config/detail <WLAN>/on <DEVICE-OR-DOMAIN-NAME>/policy-mappings/
statistics/usage-mappings}
show wireless wlan {detail <WLAN>/on <DEVICE-OR-DOMAIN-NAME>/policy-mappings/usage-
mappings}
show wireless {config filter {device <DEVICE-NAME>/rf-domain <DOMAIN-NAME>}}
show wireless wlan statistics {<WLAN>/detail/traffic} {on <DEVICE-OR-DOMAIN-NAME>}

```

## Parameters

```
show wireless ap {configured}
```

|            |                                                                                                                  |
|------------|------------------------------------------------------------------------------------------------------------------|
| wireless   | Displays wireless configuration parameters                                                                       |
| ap         | Displays managed Access Point information                                                                        |
| configured | Optional. Displays configured AP information, such as name, MAC address, profile, RF Domain and adoption status. |

```
show wireless ap {detail} {<MAC/HOST-NAME>} {(on <DEVICE-OR-DOMAIN-NAME>)}
```

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                    | Displays wireless configuration parameters                                                                                                                                                                                                                                                                                                                                                                           |
| ap                          | Displays managed Access Point information                                                                                                                                                                                                                                                                                                                                                                            |
| detail <MAC/HOST-NAME>      | Optional. Displays detailed information for all APs or a specified AP <ul style="list-style-type: none"> <li>&lt;MAC/HOST-NAME&gt; - Optional. Displays information for a specified AP. Specify the AP's MAC address.</li> </ul>                                                                                                                                                                                     |
| on <DEVICE-OR-DOMAIN-NAME>} | The following keyword is recursive and common to the 'detail <MAC/HOST-NAME>' parameters: <ul style="list-style-type: none"> <li>on &lt;DEVICE-OR-DOMAIN-NAME&gt; - Optional. Displays information on a specified device or RF Domain <ul style="list-style-type: none"> <li>&lt;DEVICE-OR-DOMAIN-NAME&gt; - Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> </li> </ul> |

```
show wireless ap {load-balancing} {client-capability|events|neighbors}
{(on <DEVICE-OR-DOMAIN-NAME>)}
```

|          |                                            |
|----------|--------------------------------------------|
| wireless | Displays wireless configuration parameters |
| ap       | Displays managed Access Point information  |

|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| load-balancing<br>{client-capability <br>events neighbors} | Optional. Displays load balancing status. Use additional filters to view specific details. <ul style="list-style-type: none"> <li>client-capability – Optional. Displays client band capability</li> <li>events – Optional. Displays client events</li> <li>neighbors – Optional. Displays neighboring clients</li> </ul>                                                                            |
| on <DEVICE-NAME>                                           | The following keyword is recursive and common to the 'client-capability', 'events', and 'neighbors' parameters: <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; – Optional. Displays load balancing information, based on the parameters passed, on a specified device</li> <li>&lt;DEVICE-NAME&gt; – Specify the name of the AP, wireless controller, or service platform.</li> </ul> |

```
show wireless bridge {candidate-ap} {<MAC/HOSTNAME> {<1-3>}}
{(filter radio-mac <RADIO-MAC>)} {(on <DEVICE-OR-DOMAIN-NAME>)}
```

|                              |                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                     | Displays wireless configuration statistics                                                                                                                                                                                                                                                                                                                        |
| bridge                       | Optional. Displays information about the candidate infrastructure access points as well as the infrastructure access point that the client-bridge radio has selected. <p><b>Note:</b> When enabled, the client-bridge radio scans its defined channels to locate the best candidate access point servicing the infrastructure WLAN.</p>                           |
| <MAC/HOSTNAME> <1-3>         | Optional. Specify the client-bridge access point's hostname or MAC address. Optionally append the radio interface's number to form client-bridge in the form of AA-BB-CC-DD-EE-FF:RX or HOSTNAME:RX. <ul style="list-style-type: none"> <li>&lt;1-3&gt; – Optional. Radio interface index if not specified as part of mesh ID.</li> </ul>                         |
| filter radio-mac <RADIO-MAC> | This is a recursive parameter and common to all of the above options. <ul style="list-style-type: none"> <li>filter radio-mac – Optional. Provides additional filters to specifically identify the radio by its MAC address</li> <li>&lt;RADIO-MAC&gt; – Specify the radio's MAC address.</li> </ul>                                                              |
| on <DEVICE-OR-DOMAIN-NAME>   | This is a recursive parameter and common to all of the above options. <ul style="list-style-type: none"> <li>on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Executes the command on a specified device or devices within a specified RF Domain</li> <li>&lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the AP, controller, service platform, or RF Domain name.</li> </ul> |

```
show wireless bridge {certificate} status {on <DEVICE-NAME>}
```

|                           |                                                                                                                                                                                 |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                  | Displays wireless configuration statistics                                                                                                                                      |
| bridge certificate status | Optional. Displays all client bridges in configuration and the status of their PKCS#12 certificates                                                                             |
| on <DEVICE-NAME>          | Optional. Executes the command on a specified device <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; – Specify the AP, controller, service platform name.</li> </ul> |

```
show wireless bridge {config}
```

|               |                                                                                                                                                                                                                   |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless      | Displays wireless configuration statistics                                                                                                                                                                        |
| bridge config | Optional. Displays all client bridges in configuration<br>The output displays the configured client-bridges' hostname, MAC address, profile, RF Domain, SSID, band, encryption, authentication, and EAP username. |

```
show wireless bridge {hosts} {on <DEVICE-OR-DOMAIN-NAME>}
```

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                   | Displays wireless configuration statistics                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| bridge hosts               | Optional. Displays the client bridge host information<br>The output displays the configured client-bridges' host's MAC Address, bridge MAC address, IPv4 address, bridging status, and activity.<br><br><b>Note:</b> The HOST MAC column displays real MAC addresses of wired hosts, while the BRIDGE MAC column displays the translated MAC addresses. The BRIDGE MAC column is based on the radio 2 base MAC address and increments by 1 for each wired host connected to the client bridges Ge1 port. |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Executes the command on a specified device or devices within a specified RF Domain. <ul style="list-style-type: none"> <li>&lt;DEVICE-OR-DOMAIN-NAME&gt; - Optional. Specify the AP, controller, service platform, or Domain name.</li> </ul>                                                                                                                                                                                                                                                  |

```
show wireless bridge {statistics} {rf|traffic} {(on <DEVICE-OR-DOMAIN-NAME>)}
```

|                            |                                                                                                                                                                                                                                                           |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                   | Displays wireless configuration statistics                                                                                                                                                                                                                |
| bridge statistics          | Optional. Displays the client-bridge related statistics                                                                                                                                                                                                   |
| rf                         | Optional. Displays the client-bridge related RF statistics<br>The output displays the signal, noise, SNR, TX/RX rates, retries, and errors.                                                                                                               |
| traffic                    | Optional. Displays the client-bridge related traffic statistics<br>The output displays TX/RX bytes, TX/RX packets, TX/RX bits/second, and dropped packets.                                                                                                |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Executes the command on a specified device or devices within a specified RF Domain <ul style="list-style-type: none"> <li>on &lt;DEVICE-OR-DOMAIN-NAME&gt; - Optional. Specify the AP, controller, service platform, or Domain name.</li> </ul> |

```
show wireless client {association-history <MAC>} {on <DEVICE-OR-DOMAIN-NAME>}
```

|                            |                                                                                                                                                                                                                                              |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                   | Displays wireless configuration parameters                                                                                                                                                                                                   |
| client                     | Displays client information based on the parameters passed                                                                                                                                                                                   |
| association-history <MAC>  | Optional. Displays association history for a specified client <ul style="list-style-type: none"> <li>&lt;MAC&gt; - Specify the MAC address of the client.</li> </ul>                                                                         |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Displays association history on a specified device or RF Domain <ul style="list-style-type: none"> <li>&lt;DEVICE-OR-DOMAIN-NAME&gt; - Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> |

```
show wireless client {detail <MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}
```



|                            |                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                   | Displays wireless configuration parameters                                                                                                                                                                                                                                                                                                                                                                             |
| client                     | Displays client information based on the parameters passed                                                                                                                                                                                                                                                                                                                                                             |
| detail <MAC>               | Optional. Displays detailed wireless client(s) information <ul style="list-style-type: none"> <li>• &lt;MAC&gt; – Optional. Displays detailed information for a specified wireless client. Specify the MAC address of the client.</li> </ul>                                                                                                                                                                           |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is recursive and common to the 'detail <MAC>' parameter: <ul style="list-style-type: none"> <li>• on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Displays detailed information on a specified device or RF Domain <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> </li> </ul> |

```
show wireless client {filter ip [<IP>/not <IP>]} {on <DEVICE-OR-DOMAIN-NAME>}
```

|                            |                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                   | Displays wireless configuration parameters                                                                                                                                                                                                                                                                                                                                         |
| client                     | Displays client information based on the parameters passed                                                                                                                                                                                                                                                                                                                         |
| filter IP [<IP>]not <IP>]  | Optional. Uses IP addresses to filter wireless clients <ul style="list-style-type: none"> <li>• &lt;IP&gt; – Selects clients with IP address matching the &lt;IP&gt; parameter</li> <li>• not &lt;IP&gt; – Inverts the match selection</li> </ul>                                                                                                                                  |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is common to the 'IP' and 'not IP' parameters: <ul style="list-style-type: none"> <li>• on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Displays selected wireless client information on a specified device or RF Domain</li> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> |

```
show wireless client {filter} {state [data-ready/not [data-ready/roaming]/roaming]} {on <DEVICE-OR-DOMAIN-NAME>}
```

|                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                                                      | Displays wireless configuration parameters                                                                                                                                                                                                                                                                                                                                                                                  |
| client                                                        | Displays client information based on the parameters passed                                                                                                                                                                                                                                                                                                                                                                  |
| filter state [data-ready  not [data-ready  roaming]] roaming] | Optional. Filters clients based on their state <ul style="list-style-type: none"> <li>• data-ready – Selects wireless clients in the data-ready state</li> <li>• not [data-ready roaming] – Inverts match selection. Selects wireless clients neither ready nor roaming</li> <li>• Roaming – Selects roaming clients</li> </ul>                                                                                             |
| on <DEVICE-OR-DOMAIN-NAME>                                    | The following keyword is common to the 'ready', 'not', and 'roaming' parameters: <ul style="list-style-type: none"> <li>• on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Displays selected client details on a specified device or RF Domain <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> </li> </ul> |

```
show wireless client {filter} {wlan [<WLAN-NAME>/not <WLAN-NAME>]} {on <DEVICE-OR-DOMAIN-NAME>}
```

|          |                                                            |
|----------|------------------------------------------------------------|
| wireless | Displays wireless configuration parameters                 |
| client   | Displays client information based on the parameters passed |

|                                            |                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| filter wlan [<WLAN-NAME>] not <WLAN-NAME>] | Optional. Filters clients on a specified WLAN <ul style="list-style-type: none"> <li>• &lt;WLAN-NAME&gt; – Specify the WLAN name.</li> <li>• not &lt;WLAN-NAME&gt; – Inverts the match selection</li> </ul>                                                                                                                                        |
| on <DEVICE-OR-DOMAIN-NAME>                 | The following keyword is common to the 'WLAN and 'not' parameters: <ul style="list-style-type: none"> <li>• on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Filters clients on a specified device or RF Domain</li> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> |

```
show wireless client {statistics} {detail <MAC>|rf|window-data <MAC>}
{(on <DEVICE-OR-DOMAIN-NAME>)}
```

|                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                                       | Displays wireless configuration parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| client                                         | Displays client information based on the parameters passed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| statistics {detail <MAC> rf window-data <MAC>} | Optional. Displays detailed client statistics. Use additional filters to view specific details. <ul style="list-style-type: none"> <li>• detail &lt;MAC&gt; – Optional. Displays detailed client statistics</li> <li>• &lt;MAC&gt; – Optional. Displays detailed statistics for a specified client. Specify the client's MAC address.</li> <li>• rf – Optional. Displays detailed RF statistics on a specified device or RF Domain</li> <li>• window-data &lt;MAC&gt; – Optional. Displays historical data, for a specified client</li> <li>• &lt;MAC&gt; – Optional. Specify the client's MAC address</li> </ul> |
| on <DEVICE-OR-DOMAIN-NAME>                     | The following keyword is recursive and common to the 'detail <MAC>', 'RF', and 'window-data <MAC>' parameters: <ul style="list-style-type: none"> <li>• on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Displays client statistics, based on the parameters passed, on a specified device or RF Domain</li> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul>                                                                                                                                                                        |

```
show wireless client {tspec} {<MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}
```

|                            |                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                   | Displays wireless configuration parameters                                                                                                                                                                                                                                                                                                                                                             |
| client                     | Displays client information based on the parameters passed                                                                                                                                                                                                                                                                                                                                             |
| tspec <MAC>                | Optional. Displays detailed TSPEC (traffic specification) information for all clients or a specified client <ul style="list-style-type: none"> <li>• &lt;MAC&gt; – Optional. Displays detailed TSPEC information for a specified client. Specify the MAC address of the client.</li> </ul>                                                                                                             |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is recursive and common to the 'tspec <MAC>' parameter: <ul style="list-style-type: none"> <li>• on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Displays detailed TSPEC information for wireless clients on a specified device or RF Domain</li> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> |

```
show wireless client {include-ipv6} {detail <MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}
```

|          |                                                            |
|----------|------------------------------------------------------------|
| wireless | Displays wireless configuration parameters                 |
| client   | Displays client information based on the parameters passed |

|                            |                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| include-ipv6               | Includes IPv6 address (if known) of wireless clients                                                                                                                                                                                                                                                                                                                         |
| detail <MAC>               | Optional. Displays detailed wireless client(s) information <ul style="list-style-type: none"> <li>• &lt;MAC&gt; - Optional. Displays detailed information for a specified wireless client. Specify the MAC address of the client.</li> </ul>                                                                                                                                 |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is recursive and common to the 'detail <MAC>' parameter: <ul style="list-style-type: none"> <li>• on &lt;DEVICE-OR-DOMAIN-NAME&gt; - Optional. Displays detailed information on a specified device or RF Domain</li> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; - Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> |

```
show wireless client {include-ipv6} {filter {ip|ipv6|state|wlan}}
```

|                                                             |                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                                                    | Displays wireless configuration parameters                                                                                                                                                                                                                                                                                                                                                          |
| client                                                      | Displays wireless client information based on the parameters passed                                                                                                                                                                                                                                                                                                                                 |
| include-ipv6 {filter}                                       | Optional. Includes IPv6 address (if known) of wireless clients <ul style="list-style-type: none"> <li>• filter - Optional. Defines additional filters. Use one of the following options to filter clients: ip, ipv6, state, and wlan.</li> </ul> <p>By default the system only displays the IPv4 address of clients. The include-ipv6 parameter includes the known IPv6 address of each client.</p> |
| ip [<IPv4> not <IPv4>]                                      | Optional. Displays wireless client information based on the IPv4 address passed <ul style="list-style-type: none"> <li>• &lt;IPv4&gt; - Displays information of the client identified by the &lt;IPv4&gt; parameter</li> <li>• not &lt;IPv4&gt; - Inverts the match selection</li> </ul>                                                                                                            |
| ipv6 [<IPv6> not <Pv6>]                                     | Optional. Displays wireless client information based on the IPv6 address passed <ul style="list-style-type: none"> <li>• &lt;IPv6&gt; - Displays information of the client identified by the &lt;IPv6&gt; parameter</li> <li>• not &lt;IPv6&gt; - Inverts the match selection</li> </ul>                                                                                                            |
| filter state [data-ready] not [data-ready roaming] roaming] | Optional. Filters wireless client information based on their state <ul style="list-style-type: none"> <li>• data-ready - Displays information of wireless clients in the data-ready state</li> <li>• not [data-ready roaming] - Inverts match selection. Displays information of wireless clients neither ready nor roaming</li> <li>• Roaming - Displays information of roaming clients</li> </ul> |
| wlan [<WLAN-NAME> not <WLAN-NAME>]                          | Optional. Displays wireless client information based on the WLAN name passed <ul style="list-style-type: none"> <li>• &lt;WLAN-NAME&gt; - Specify the WLAN name.</li> <li>• not &lt;WLAN-NAME&gt; - Inverts match selection</li> </ul>                                                                                                                                                              |

```
show wireless coverage-hole-incidents {detail} {filter [ap <MAC/HOSTNAME>|client-mac <MAC>]|summary} {(on <DOMAIN-NAME>)}
```

|                         |                                                                                                                                                                               |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                | Displays wireless configuration parameters. Use this option to view coverage-hole related incidents encountered by wireless clients and reported to associated access points. |
| coverage-hole-incidents | Displays coverage-hole related statistics                                                                                                                                     |

|                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| detail filters [ap <MAC/<br>HOSTNAME>  client-mac<br><MAC>] | <p>Optional. Displays detailed coverage-hole related statistics</p> <ul style="list-style-type: none"> <li>filters - Optional. Displays detailed coverage-hole related statistics on a per access point or wireless-client basis <ul style="list-style-type: none"> <li>ap &lt;MAC/HOSTNAME&gt; - Displays detailed coverage-hole related statistics for a specified access point<br/>&lt;MAC/HOSTNAME&gt; - Specify the access point's device name or MAC address.</li> <li>client-mac &lt;MAC&gt; - Displays detailed coverage-hole related statistics encountered by a specified wireless client<br/>&lt;MAC&gt; - Specify the wireless client's MAC address</li> </ul> </li> </ul> <p><b>Note:</b> If the command is executed without any parameters being included, the system displays all coverage-hole related statistics.</p> |
| summary                                                     | Optional. Displays a summary of coverage-hole related statistics                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| on <DOMAIN-NAME>                                            | <p>This parameter is recursive and is common to the 'detail' and 'summary' keywords:</p> <ul style="list-style-type: none"> <li>on &lt;DOMAIN-NAME&gt; - Optional. Displays detailed or summary coverage-hole related statistics on a specified RF Domain</li> <li>&lt;DOMAIN-NAME&gt; - Specify the domain name.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

```
show wireless meshpoint {config} {filter [device <DEVICE-NAME>|rf-domain <DOMAIN-NAME>]}
```

|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                                                | Displays wireless configuration parameters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| meshpoint                                               | <p>Displays meshpoint related information</p> <p>Use this option to view detailed statistics on each Mesh-capable client available within controller's adopted access point's radio coverage area.</p> <p>A mesh network is where one where each node is able to communicate with other nodes and maintain more than one path to the other mesh nodes within the mesh network. A mesh network provides robust, reliable and redundant connectivity to all the members of the mesh network. When one member of the mesh network becomes unavailable, the other mesh nodes are still able to communicate with one another either directly or indirectly through intermediate nodes.</p> |
| config                                                  | Optional. Displays all meshpoint configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| filters [device <DEVICE-NAME>  rf-domain <DOMAIN-NAME>] | <p>Optional. Provides additional filter options, such as device name and RF Domain name.</p> <ul style="list-style-type: none"> <li>device &lt;DEVICE-NAME&gt; - Displays meshpoints applied to a specified device <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; - Specify the device name</li> </ul> </li> <li>rf-domain &lt;DOMAIN-NAME&gt; - Displays meshpoints applied to a specified RF Domain <ul style="list-style-type: none"> <li>&lt;DOMAIN-NAME&gt; - Specify the domain name</li> </ul> </li> </ul>                                                                                                                                                         |

```
show wireless meshpoint {detail} {<MESHPOINT-NAME>}
```

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                   | Displays wireless configuration parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| meshpoint                  | Displays meshpoint related information<br>Use this option to view detailed statistics on each Mesh-capable client available within controller's adopted access point's radio coverage area.<br>A mesh network is where one where each node is able to communicate with other nodes and maintain more then one path to the other mesh nodes within the mesh network. A mesh network provides robust, reliable and redundant connectivity to all the members of the mesh network. When one member of the mesh network becomes unavailable, the other mesh nodes are still able to communicate with one another either directly or indirectly through intermediate nodes. |
| detail<br><MESHPOINT-NAME> | Optional. Displays detailed information for all meshpoints or a specified meshpoint <ul style="list-style-type: none"> <li>• &lt;MESHPOINT-NAME&gt; - Optional. Displays detailed information for a specified meshpoint. Specify the meshpoint name.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                        |

```
show wireless meshpoint {multicast/path/proxy/root/security/statistics}
[<MESHPOINT-NAME>|detail] {on <DEVICE-OR-DOMAIN-NAME>}
```

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                   | Displays wireless configuration parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| meshpoint                  | Displays meshpoint related information<br>Use this option to view detailed statistics on each Mesh-capable client available within controller's adopted access point's radio coverage area.<br>A mesh network is where one where each node is able to communicate with other nodes and maintain more then one path to the other mesh nodes within the mesh network. A mesh network provides robust, reliable and redundant connectivity to all the members of the mesh network. When one member of the mesh network becomes unavailable, the other mesh nodes are still able to communicate with one another either directly or indirectly through intermediate nodes. |
| multicast                  | Optional. Displays meshpoint multicast information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| path                       | Optional. Displays meshpoint path information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| proxy                      | Optional. Displays meshpoint proxy information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| root                       | Optional. Displays meshpoint root information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| security                   | Optional. Displays meshpoint security information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| statistics                 | Optional. Displays meshpoint statistics                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| [<MESHPOINT-NAME> detail]  | The following keywords are common to all of the above parameters: <ul style="list-style-type: none"> <li>• &lt;MESHPOINT-NAME&gt; - Displays meshpoint related information for a specified meshpoint. Specify the meshpoint name.</li> <li>• detail - Displays detailed multicast information for all meshpoints</li> </ul>                                                                                                                                                                                                                                                                                                                                            |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is common to all of the above parameters: <ul style="list-style-type: none"> <li>• on &lt;DEVICE-OR-DOMAIN-NAME&gt; - Optional. Displays detailed multicast information on a specified device or RF Domain. <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; - Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> </li> </ul>                                                                                                                                                                                                                                                     |

```
show wireless meshpoint {neighbor} [<MESHPOINT-NAME>|detail|statistics {rf}]
{on <DEVICE-OR-DOMAIN-NAME>}
```

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                                    | Displays wireless configuration parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| meshpoint                                   | Displays meshpoint related information<br>Use this option to view detailed statistics on each Mesh-capable client available within controller's adopted access point's radio coverage area.<br>A mesh network is where one where each node is able to communicate with other nodes and maintain more than one path to the other mesh nodes within the mesh network. A mesh network provides robust, reliable and redundant connectivity to all the members of the mesh network. When one member of the mesh network becomes unavailable, the other mesh nodes are still able to communicate with one another either directly or indirectly through intermediate nodes. |
| neighbor                                    | Optional. Displays meshpoint neighbor information, based on the parameters passed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| [<MESHPOINT-NAME>  detail  statistics {rf}] | Select one of the following parameter to view neighbor related information <ul style="list-style-type: none"> <li>• &lt;MESHPOINT-NAME&gt; – Displays detailed multicast information for a specified meshpoint. Specify the meshpoint name.</li> <li>• detail – Displays detailed multicast information for all meshpoints</li> <li>• statistics – Displays neighbors related statistics <ul style="list-style-type: none"> <li>• rf – Optional. Displays RF related statistics for neighbors</li> </ul> </li> </ul>                                                                                                                                                   |
| on <DEVICE-OR-DOMAIN- NAME>                 | The following keyword is common to all of the above parameters: <ul style="list-style-type: none"> <li>• on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Displays meshpoint neighbor information, based on the parameters passed, on a specified device or RF Domain.</li> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul>                                                                                                                                                                                                                                                              |

```
show wireless meshpoint {tree} {on <DEVICE-OR-DOMAIN- NAME>}
```

|                            |                                                                                                                                                                                                                                                        |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                   | Displays wireless configuration parameters                                                                                                                                                                                                             |
| meshpoint                  | Displays meshpoint related information<br><br><b>Note:</b> The <b>show &gt; wireless &gt; meshpoint &gt; tree</b> command can be executed only from a wireless controller.                                                                             |
| tree                       | Optional. Displays meshpoint network tree                                                                                                                                                                                                              |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Displays meshpoint network tree on a specified device or RF Domain <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Specify the name of AP, wireless controller, service platform, or RF Domain</li> </ul> |

```
show wireless meshpoint {usage-mappings/on <DEVICE-OR-DOMAIN-NAME>}
```

|                            |                                                                                                                                                                                                                                                   |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                   | Displays wireless configuration parameters                                                                                                                                                                                                        |
| meshpoint                  | Displays meshpoint related information                                                                                                                                                                                                            |
| usage-mappings             | Optional. Lists all devices and profiles using the meshpoint                                                                                                                                                                                      |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Displays meshpoint applied to a specified device or RF Domain <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Specify the name of AP, wireless controller, service platform, or RF Domain</li> </ul> |

```
show wireless mobility-database {on <DEVICE-OR-DOMAIN-NAME>}
```

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                   | Displays wireless configuration parameters                                                                                                                                                                                                                                                                                                                                                                              |
| mobility-database          | Displays controller-assisted mobility database                                                                                                                                                                                                                                                                                                                                                                          |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is recursive and common to the 'filter <RADIO-MAC>' parameter: <ul style="list-style-type: none"> <li>on &lt;DEVICE-OR-DOMAIN-NAME&gt; - Optional. Displays detailed radio operation status for all or a specified radio on a specified device or RF Domain.</li> <li>&lt;DEVICE-OR-DOMAIN-NAME&gt; - Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> |

```
show wireless mint [client|detail] {portal-candidates {<DEVICE-NAME>}/
filter <RADIO-MAC>}/statistics} (on <DEVICE-OR-DOMAIN-NAME>)
```

|                               |                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless mint [client detail] | Displays radio MiNT-mesh related statistics <ul style="list-style-type: none"> <li>client - Displays MiNT-mesh client related information. Use the 'client' option to view detailed statistics on each Mesh capable client available within the selected access point's radio coverage area.</li> <li>detail - Displays detailed MiNT-mesh related information</li> </ul>        |
| portal-candidates             | Displays detailed information about portal candidates for a MiNT-mesh. Mesh points connected to an external network and forwarding traffic in and out are Mesh portals. Mesh points must find paths to a portal to access the Internet. When multiple portals exist, the mesh point must select one. Use the additional filter option to view specific portal candidate details. |
| statistics                    | This option is common to the 'client' and 'detail' keyword. Displays MiNT-mesh client statistical data.                                                                                                                                                                                                                                                                          |
| on <DEVICE-OR-DOMAIN-NAME>    | This option is common to the 'client' and 'detail' keyword. Displays MiNT-mesh client related information on a specific device or RF Domain <ul style="list-style-type: none"> <li>&lt;DEVICE-OR-DOMAIN-NAME&gt; - Specify the access point, controller, or RF Domain name.</li> </ul>                                                                                           |

```
show wireless mint portal statistics {on <DEVICE-OR-DOMAIN-NAME>}
```

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless mint              | Displays radio MiNT-mesh related statistics                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| links                      | Displays MiNT-mesh links related information. MiNT Links are automatically created between controllers and access points during adoption using MLCP (MiNT Link Creation Protocol). They can also be manually created between a controller and access point (or) between access points. MiNT links are manually created between controllers while configuring a cluster. Level 2 (or) remote MiNT links are controller aware links, and requires IP network for communication. This level 2 MiNT links at access points are intended for remote adaptive AP deployment and management from NOC. With Level2 MiNT links, access points are only aware of the controllers and not about other access points. Level 2 MiNT links also provide partitioning, between access points deployed at various remote sites. |
| on <DEVICE-OR-DOMAIN-NAME> | Displays MiNT-mesh links on a specific device or RF Domain <ul style="list-style-type: none"> <li>&lt;DEVICE-OR-DOMAIN-NAME&gt; - Specify the access point, controller, or RF Domain name.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

```
show wireless mint portal statistics {on <DEVICE-OR-DOMAIN-NAME>}
```

|                            |                                                                                                                                                                                                                           |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless mint              | Displays radio MiNT-mesh related statistics                                                                                                                                                                               |
| portal                     | Displays legacy client on MiNT-mesh portal                                                                                                                                                                                |
| on <DEVICE-OR-DOMAIN-NAME> | Displays legacy client on MiNT-mesh portal on a specific device or RF Domain <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the access point, controller, or RF Domain name.</li> </ul> |

```
show wireless radio {detail} {<DEVICE-NAME> {<1-3>/filter/on}}
```

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                   | Displays wireless configuration parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| radio                      | Displays radio operation status and other related information. Use this option to view radio association data, including radio ID, connected APs, radio type, quality index and SNR (Signal to Noise Ratio). This data is reported to the managing controller or service platform from connected access point radios and should be refreshed periodically.<br>A radio's RF Mode displays as: <ul style="list-style-type: none"> <li>• 2.4GHz-wlan – If it is configured to provide 2.4 GHz WLAN service</li> <li>• 5GHz-wlan – If it is configured to provide 5.0 GHz WLAN service</li> <li>• bridge – If it is configured to provide client-bridge operation</li> </ul> |
| detail                     | Optional. Displays detailed radio operation status                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <DEVICE-NAME>              | Optional. Displays detailed information for a specified radio. Specify the MAC address or hostname, or append the interface number to form the radio ID in the AA-BB-CC-DD-EE-FF:RX or HOSTNAME:RX format.                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <1-3>                      | Optional. Specify the radio interface index from 1 - 3 (if not specified as part of the radio ID)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| filter <RADIO-MAC>         | Optional. Provides additional filters <ul style="list-style-type: none"> <li>• &lt;RADIO-MAC&gt; – Optional. Filters based on the radio MAC address</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. After specifying the radio MAC address, further refine the search by specifying a device or RF Domain. <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                    |

```
show wireless radio {detail} {filter <RADIO-MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}
```

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless | Displays wireless configuration parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| radio    | Displays radio operation status and other related information. Use this option to view radio association data, including radio ID, connected APs, radio type, quality index and SNR. This data is reported to the managing controller or service platform from connected access point radios and should be refreshed periodically.<br>A radio's RF Mode displays as: <ul style="list-style-type: none"> <li>• 2.4GHz-wlan – If it is configured to provide 2.4 GHz WLAN service</li> <li>• 5GHz-wlan – If it is configured to provide 5.0 GHz WLAN service</li> <li>• bridge – If it is configured to provide client-bridge operation</li> </ul> |
| detail   | Optional. Displays detailed radio operation status                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |



|                            |                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| filter <RADIO-MAC>         | Optional. Provides additional filter options <ul style="list-style-type: none"> <li>• &lt;RADIO-MAC&gt; – Uses MAC address to filter radios</li> </ul>                                                                                                                                                                                                                                                                      |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is recursive and common to the 'filter <RADIO-MAC>' parameter: <ul style="list-style-type: none"> <li>• on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Displays detailed radio operation status for all or a specified radio on a specified device or RF Domain.</li> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> |

```
show wireless radio {statistics} {on <DEVICE-OR-DOMAIN-NAME>}/rf {on <DEVICE-OR-DOMAIN-NAME>}}
```

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                        | Displays wireless configuration parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| radio                           | Displays radio operation status and other related information. Use this option to view radio association data, including radio ID, connected APs, radio type, quality index and SNR. This data is reported to the managing controller or service platform from connected access point radios and should be refreshed periodically.<br>A radio's RF Mode displays as: <ul style="list-style-type: none"> <li>• 2.4GHz-wlan – If it is configured to provide 2.4 GHz WLAN service</li> <li>• 5GHz-wlan – If it is configured to provide 5.0 GHz WLAN service</li> <li>• bridge – If it is configured to provide client-bridge operation</li> </ul> |
| statistics                      | Optional. Displays radio traffic and RF statistics                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| on <DEVICE-OR-DOMAIN-NAME>      | Optional. Displays traffic and RF related statistics on a specified device or RF Domain <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                     |
| rf {on <DEVICE-OR-DOMAIN-NAME>} | Optional. Displays RF statistics on a specified device or RF Domain <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                         |

```
show wireless radio {statistics} {detail/window-data} {<DEVICE-NAME>} {<1-3>}/filter <RADIO-MAC> { (on <DEVICE-OR-DOMAIN-NAME>) }
```

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                        | Displays wireless configuration parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| radio                           | Displays radio operation status and other related information. Use this option to view radio association data, including radio ID, connected APs, radio type, quality index and SNR. This data is reported to the managing controller or service platform from connected access point radios and should be refreshed periodically.<br>A radio's RF Mode displays as: <ul style="list-style-type: none"> <li>• 2.4GHz-wlan – If it is configured to provide 2.4 GHz WLAN service</li> <li>• 5GHz-wlan – If it is configured to provide 5.0 GHz WLAN service</li> <li>• bridge – If it is configured to provide client-bridge operation</li> </ul> |
| statistics {detail/window-data} | Optional. Displays radio traffic and RF statistics. Use additional filters to view specific details. The options are: <ul style="list-style-type: none"> <li>• detail – Displays detailed traffic and RF statistics of all radios</li> <li>• window-data – Displays historical data over a time-window</li> </ul>                                                                                                                                                                                                                                                                                                                                |
| <1-3>                           | Optional. Specify the radio interface index from 1- 3, if not specified as part of the radio ID using the preceding parameter.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

|                            |                                                                                                                                                                                                                                                                                       |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| filter <RADIO-MAC>         | Optional. Provides additional filters <ul style="list-style-type: none"> <li>• &lt;RADIO-MAC&gt; – Optional. Filters based on the radio MAC address</li> </ul>                                                                                                                        |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. After specifying the radio MAC address, further refine the search by specifying a device or RF Domain. <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> |

```
show wireless radio {tspec} {<DEVICE-NAME>|filter|on <DEVICE-OR-DOMAIN-NAME>|option}
```

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                   | Displays wireless configuration parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| radio                      | Displays radio operation status and other related information. Use this option to view radio association data, including radio ID, connected APs, radio type, quality index and SNR. This data is reported to the managing controller or service platform from connected access point radios and should be refreshed periodically.<br>A radio's RF Mode displays as: <ul style="list-style-type: none"> <li>• 2.4GHz-wlan – If it is configured to provide 2.4 GHz WLAN service</li> <li>• 5GHz-wlan – If it is configured to provide 5.0 GHz WLAN service</li> <li>• bridge – If it is configured to provide client-bridge operation</li> </ul> |
| tspec                      | Optional. Displays TSPEC information on a radio                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <DEVICE-NAME>              | Optional. Specify the MAC address or hostname, or append the interface number to form the radio ID in the AA-BB-CC-DD-EE-FF:RX or HOSTNAME:RX format.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| filter                     | Optional. Provides additional filters <ul style="list-style-type: none"> <li>• &lt;RADIO-MAC&gt; – Optional. Filters based on the radio MAC address</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. After specifying the radio MAC address, further refine the search by specifying a device or RF Domain. <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul>                                                                                                                                                                                                                                                                                                                                                            |

```
show wireless regulatory [channel-info <WORD>|country-code <WORD>]
```

|                     |                                                                                                                                                                    |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless            | Displays wireless configuration parameters                                                                                                                         |
| regulatory          | Displays wireless regulatory information                                                                                                                           |
| channel-info <WORD> | Displays channel information <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the channel number.</li> </ul>                                        |
| country-code <WORD> | Displays country code to country name information <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the two letter ISO-3166 country code.</li> </ul> |

```
show wireless regulatory device-type [ap6522|ap6562|ap7161|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap8163|ap8432|ap8533] <WORD>
```

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                            | Displays wireless configuration parameters                                                                                                                                                                                                                                                                                                                                                                                                    |
| regulatory                          | Displays wireless regulatory information                                                                                                                                                                                                                                                                                                                                                                                                      |
| device-type <DEVICE-TYPE><br><WORD> | Displays wireless regulatory information based on the device type selected. Select the device type. The options are:<br>AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533<br>After specifying the device type, specify the country code. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specify the two letter ISO-3166 country code.</li> </ul> |

```
show wireless rf-domain statistics {detail} {(on <DEVICE-OR-DOMAIN-NAME>)}
```

|                            |                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                   | Displays wireless configuration parameters                                                                                                                                                                                                                                                                                                                             |
| rf-domain statistics       | Displays RF Domain statistics                                                                                                                                                                                                                                                                                                                                          |
| details                    | Optional. Displays detailed RF Domain statistics                                                                                                                                                                                                                                                                                                                       |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is recursive and common to the 'detail' parameter: <ul style="list-style-type: none"> <li>• on &lt;DEVICE-OR-DOMAIN-NAME&gt; - Optional. Displays RF Domain statistics on a specified device or RF Domain</li> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; - Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> |

```
show wireless sensor-server {on <DEVICE-OR-DOMAIN-NAME>}
```

|                                              |                                                                                                                                                                                                                                             |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                                     | Displays wireless configuration parameters                                                                                                                                                                                                  |
| sensor- server {on <DEVICE-OR-DOMAIN- NAME>} | Displays AirDefense sensor server configuration details <ul style="list-style-type: none"> <li>• on &lt;DEVICE-OR-DOMAIN-NAME&gt; - Optional. Displays AirDefense sensor server configuration on a specified device or RF Domain</li> </ul> |

```
show wireless unsanctioned aps {detailed/statistics} {(on <DEVICE-OR-DOMAIN-NAME>)}
```

|                             |                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                    | Displays wireless configuration parameters                                                                                                                                                                                                                                                                                                                                                   |
| unsanctioned aps            | Displays unauthorized APs. Use additional filters to view specific details.                                                                                                                                                                                                                                                                                                                  |
| detailed                    | Optional. Displays detailed unauthorized APs information                                                                                                                                                                                                                                                                                                                                     |
| statistics                  | Optional. Displays channel statistics                                                                                                                                                                                                                                                                                                                                                        |
| on <DEVICE-OR-DOMAIN- NAME> | The following keyword is common to the 'detailed' and 'statistics' parameters: <ul style="list-style-type: none"> <li>• on &lt;DEVICE-OR-DOMAIN-NAME&gt; - Optional. Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; - Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> |

```
show wireless wips [client-blacklist|event-history] {on <DEVICE-OR-DOMAIN-NAME>}
```

|                                       |                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                              | Displays wireless configuration parameters                                                                                                                                                                                                                                                                                                                                       |
| wips [client-blacklist event-history] | Displays the WIPS details <ul style="list-style-type: none"> <li>client-blacklist – Displays blacklisted clients</li> <li>event-history – Displays event history</li> </ul>                                                                                                                                                                                                      |
| on <DEVICE-OR-DOMAIN-NAME>            | The following keyword is common to the 'client-blacklist' and 'event-history' parameters: <ul style="list-style-type: none"> <li>on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Optional. Displays the WIPS details on a specified device or RF Domain.</li> <li>&lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> |

`show wlan {detail <WLAN>/on <DEVICE-OR-DOMAIN-NAME>/policy-mappings/usage-mappings}`

|                            |                                                                                                                                                                                                                                             |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                   | Displays wireless configuration parameters                                                                                                                                                                                                  |
| wlan                       | Displays WLAN related information based on the parameters passed                                                                                                                                                                            |
| detail <WLAN>              | Optional. Displays WLAN configuration <ul style="list-style-type: none"> <li>&lt;WLAN&gt; – Specify the WLAN name.</li> </ul>                                                                                                               |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Displays WLAN configuration on a specified device or RF Domain <ul style="list-style-type: none"> <li>&lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> |
| policy-mappings            | Optional. Displays WLAN policy mappings                                                                                                                                                                                                     |
| usage-mappings             | Optional. Lists all devices and profiles using the WLAN                                                                                                                                                                                     |

`show wlan {config filter {device <DEVICE-NAME>/rf-domain <DOMAIN-NAME>}}`

|                         |                                                                                                                                                               |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                | Displays wireless configuration parameters                                                                                                                    |
| wlan                    | Displays WLAN related information based on the parameters passed                                                                                              |
| config filter           | Optional. Filters WLAN information based on the device name or RF Domain                                                                                      |
| device <DEVICE-NAME>    | Optional. Filters WLAN information based on the device name <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; – Specify the device name.</li> </ul>  |
| rf-domain <DOMAIN-NAME> | Optional. Filters WLAN information based on the RF Domain <ul style="list-style-type: none"> <li>&lt;DOMAIN-NAME&gt; – Specify the RF Domain name.</li> </ul> |

`show wlan {detail <WLAN>/on <DEVICE-OR-DOMAIN-NAME>/policy-mappings/usage-mappings}`

|                            |                                                                                                                                                                                                                                             |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                   | Displays wireless configuration parameters                                                                                                                                                                                                  |
| wlan                       | Displays WLAN related information based on the parameters passed                                                                                                                                                                            |
| detail <WLAN>              | Optional. Displays WLAN configuration <ul style="list-style-type: none"> <li>&lt;WLAN&gt; – Specify the WLAN name.</li> </ul>                                                                                                               |
| on <DEVICE-OR-DOMAIN-NAME> | Optional. Displays WLAN configuration on a specified device or RF Domain <ul style="list-style-type: none"> <li>&lt;DEVICE-OR-DOMAIN-NAME&gt; – Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> |

|                 |                                                         |
|-----------------|---------------------------------------------------------|
| policy-mappings | Optional. Displays WLAN policy mappings                 |
| usage-mappings  | Optional. Lists all devices and profiles using the WLAN |

```
show wlan {config filter {device <DEVICE-NAME>|rf-domain <DOMAIN-NAME>}}
```

|                         |                                                                                                                                                              |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                | Displays wireless configuration parameters                                                                                                                   |
| wlan                    | Displays WLAN related information based on the parameters passed                                                                                             |
| config filter           | Optional. Filters WLAN information based on the device name or RF Domain                                                                                     |
| device <DEVICE-NAME>    | Optional. Filters WLAN information based on the device name <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; - Specify the device name.</li> </ul> |
| rf-domain <DOMAIN-NAME> | Optional. Filters WLAN information based on the RF Domain <DOMAIN-NAME> - Specify the RF Domain name.                                                        |

```
show wlan {statistics {<WLAN>|detail} {(on <DEVICE-OR-DOMAIN-NAME>)}}
```

|                            |                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless                   | Displays wireless configuration parameters                                                                                                                                                                                                                                                                                                                                                            |
| wlan                       | Displays WLAN related information based on the parameters passed                                                                                                                                                                                                                                                                                                                                      |
| statistics {<WLAN> detail} | Optional. Displays WLAN statistics. Use additional filters to view specific details <ul style="list-style-type: none"> <li>&lt;WLAN&gt; - Optional. Displays WLAN statistics. Specify the WLAN name.</li> <li>detail - Optional. Displays detailed WLAN statistics</li> </ul>                                                                                                                         |
| on <DEVICE-OR-DOMAIN-NAME> | The following keyword is common to the 'WLAN' and 'detail' parameters: <ul style="list-style-type: none"> <li>on &lt;DEVICE-OR-DOMAIN-NAME&gt; - Optional. Displays WLAN statistics on a specified device or RF Domain <ul style="list-style-type: none"> <li>&lt;DEVICE-OR-DOMAIN-NAME&gt; - Specify the name of the AP, wireless controller, service platform, or RF Domain.</li> </ul> </li> </ul> |

## Examples

```
nx9500-6C8809(config)#show wireless wlan config
```

```

NAME ENABLE SSID ENCRYPTION AUTHENTICATION VLAN BRIDGING MODE

test Y test wep64 none 1 local

```

```
nx9500-6C8809(config)#
```

```
nx9500-6C8809(config)#show wireless wips client-blacklist
```

```
No wireless clients blacklisted
```

```
nx9500-6C8809(config)#
```

```
nx9500-6C8809(config)#show wireless regulatory country-code
```

```

ISO CODE NAME

gt Guatemala
co Colombia
cn China
cm Cameroon
cl Chile

```

```
--More--
```

```
nx9500-6C8809(config)#
```

```
nx9500-6C8809(config)#show wireless regulatory device-type ap7502 us
```

```

```

| # | Channel Set | Power(mW) | Power (dBm) | Placement      | DFS          | CAC(mins) | TPC          |
|---|-------------|-----------|-------------|----------------|--------------|-----------|--------------|
| 1 | 1-11        | 4000      | 36          | Indoor/Outdoor | NA           | NA        | NA           |
| 2 | 36-48       | 4000      | 36          | Indoor/Outdoor | Not Required | 0         | Not Required |
| 3 | 52-64       | 500       | 27          | Indoor/Outdoor | Required     | 1         | Not Required |
| 4 | 52-64       | 1000      | 30          | Indoor/Outdoor | Required     | 1         | Required     |
| 5 | 100-140     | 500       | 27          | Indoor/Outdoor | Required     | 1         | Not Required |
| 6 | 100-140     | 1000      | 30          | Indoor/Outdoor | Required     | 1         | Required     |
| 7 | 149-165     | 4000      | 36          | Indoor/Outdoor | Not Required | 0         | Not Required |

```

nx9500-6C8809(config)#
nx9600-7F5124#show wireless meshpoint tree on PTP-AP
In progress
1:PTP-Radio2 [7 MPs(2 roots, 5 bound)]
|-ap7562-84A484-ROOT1
| |-ap7562-84A2CC-VMM
| |-ap7532-80C28C-NR
| |-ap7532-82CCA4-NR
| |-ap7562-84A22C-NR2
| |-ap7532-160114
|-ap7562-84A280-ROOT2

```

```

Total number of meshes displayed: 1
nx9600-7F5124#
ap6532-000001#show wireless meshpoint multicast detail
Multicast Paths @00-23-68-00-00-01 (ap6532-000001), mesh1 [00-23-68-2E-64-B2]

```

| Group-Addr        | Subscriber Name | Subscriber MPID   | Timeout (mSecs) |
|-------------------|-----------------|-------------------|-----------------|
| 01-00-5E-01-01-01 | ap6532-000001   | 00-23-68-2E-64-B2 | N/A             |

```

Total number of meshpoint displayed: 1
ap6532-000001#
ap6532-000001#show wireless meshpoint neighbor detail
Neighbors @00-23-68-00-00-01 (ap6532-000001), mesh1 [00-23-68-2E-64-B2]

```

| Neighbor Name Type | Neighbor MPID.Interface | IFID Auth-State                                 | Root Name LQ% | Root MPID LMet       | RMet Hops |
|--------------------|-------------------------|-------------------------------------------------|---------------|----------------------|-----------|
| Fixed              | 00-23-68-00-00-01:R2    | 5C-0E-8B-21-76-22.5C-0E-8B-21-74-40 Enabled Yes | 0 97 87       | 00-23-68-2E-97-60 20 | 115 1     |
| Fixed              | 00-23-68-00-00-01:R2    | 00-23-68-30-F7-82.00-23-68-30-F8-F0 Init Yes    | 0 97 86       | 00-23-68-2E-97-60 30 | 99 1      |
| Fixed              | 00-23-68-00-00-01:R1    | 00-23-68-30-F7-82.00-23-68-30-F7-82 Enabled Yes | 0 96 94       | 00-23-68-2E-97-60 0  | 99 1      |
| Fixed              | 00-23-68-00-00-01:R1    | 5C-0E-8B-21-76-22.5C-0E-8B-21-76-22 Enabled Yes | 0 96 93       | 00-23-68-2E-97-60 30 | 115 1     |
| Root               | 00-23-68-00-00-01:R2    | 00-23-68-2E-AB-50.00-23-68-2E-AB-50 Enabled Yes | 7 96 87       | 00-23-68-2E-AB-50 40 | 0 0       |
| Root               | 00-23-68-00-00-01:R2    | 00-23-68-2E-97-60.00-23-68-2E-97-60 Enabled Yes | 8 94 90       | 00-23-68-2E-97-60 10 | 0 0       |

```
Total number of meshpoint displayed: 1
ap6532-000001#
ap6532-000001#show wireless meshpoint proxy detail
Proxies @00-23-68-00-00-01 (ap6532-000001), mesh1 [00-23-68-2E-64-B2]
```

| Destination Addr  | Owner Name    | Owner MPID        | Persist   | VLAN | Age       |
|-------------------|---------------|-------------------|-----------|------|-----------|
| 00-23-68-00-00-01 | ap6532-000001 | 00-23-68-2E-64-B2 | Permanent | 101  | 180654310 |
| 00-1E-E5-A6-66-E2 | ap6532-000001 | 00-23-68-2E-64-B2 | Untimed   | 103  | 231920    |

```
Total number of meshpoint displayed: 1
ap6532-000001#
ap6532-000001#show wireless meshpoint multicast mesh1
Multicast Paths @00-23-68-00-00-01 (ap6532-000001), mesh1 [00-23-68-2E-64-B2]
```

| Group-Addr        | Subscriber Name | Subscriber MPID   | Timeout (mSecs) |
|-------------------|-----------------|-------------------|-----------------|
| 01-00-5E-01-01-01 | ap6532-000001   | 00-23-68-2E-64-B2 | -1              |

```
Total number of meshpoint displayed: 1
ap6532-000001#
ap6532-000001#show wireless meshpoint path detail
Paths @00-23-68-00-00-01 (ap6532-000001), mesh1 [00-23-68-2E-64-B2]
```

| Destination Name | Destination Addr | Next Hop Name | Next Hop IFID | State | Hops        | Type              | Binding                        |
|------------------|------------------|---------------|---------------|-------|-------------|-------------------|--------------------------------|
| Metric           | Timeout          | Path-Timeout  | Sequence      | MinT  | ID          |                   |                                |
| Bound            | 89               | 8730          | 0             | 23847 | 68.31.19.58 | 00-23-68-2E-AB-50 | 00-23-68-2E-AB-50 Valid 1 Root |
| Unbound          | 92               | 5200          | 0             | 3481  | 68.31.1A.80 | 00-23-68-2E-97-60 | 00-23-68-2E-97-60 Valid 1 Root |

```
ap6532-000001#
rfs4000-22A24E#show wireless client
```

```
Report start on RF-Domain: qsl
MAC IP VENDOR RADIO-ID
WLAN VLAN STATE
```

```
Report end on RF-Domain: qsl
```

```
Report start on RF-Domain: Store-1
MAC IP VENDOR RADIO-ID
WLAN VLAN STATE
```

```
00-01-02-03-04-10 2.3.4.16 3Com Corp 00-01-02-03-04-00:R1 sim-
wlan-1 1 Data-Ready
00-01-02-03-05-10 2.3.5.16 3Com Corp 00-01-02-03-04-00:R2 sim-
wlan-1 1 Data-Ready
Report end on RF-Domain: Store-1
```

```


Report start on RF-Domain: default
 database not available
Report end on RF-Domain: default


```

```

Total number of clients displayed: 2
rfs4000-22A24E#

```

The following examples show client-bridge related information:

```

NX9500(config)#show adoption status

```

```

DEVICE-NAME VERSION CFG-STAT MSGS ADOPTED-BY LAST-ADOPTION UPTIME

ap6562-167598 5.9.1.0-017DB configured No NX9500 0 days 00:01:59 0 days 00:03:22

```

```

Total number of devices displayed: 1

```

```

NX9500(config)#
NX9500(config)#show wireless bridge on ap6562-167598

```

```

LOCAL RADIO LOCAL BSSID SELECTED AP RF-BAND CHANNEL STATE UP TIME
ACTIVITY
(sec ago)

ap6562-167598:R2 FC-0A-81-16-69-50 B4-C7-99-CA-A1-F0 5GHz 104 Selected 0 days
00:01:55 00:00:00

```

```

Total number of radios displayed: 1

```

```

NX9500(config)#
NX9500(config)#show wireless bridge config

```

```

IDX NAME MAC PROFILE RF-DOMAIN SSID
BAND ENCRYPTION AUTHENTICATION EAP-USERNAME

1 ap6562-167598 FC-0A-81-16-75-98 default-ap6562 default inf_ap 2.4GHz/
5GHz ccmp eap hoabeo

```

```

NX9500(config)#
NX9500(config)#show wireless bridge hosts

```

```

HOST MAC BRIDGE MAC IP BRIDGING STATUS ACTIVITY
(sec ago)

FC-0A-81-16-75-98 FC-0A-81-16-69-50 172.16.34.55 UP 00:00:00

```

```

Total number of hosts displayed: 1

```

```

NX9500(config)#
NX9500(config)#show wireless bridge statistics

```

```

LOCAL RADIO CONNECTED AP SIGNAL SNR TX-RATE RX-RATE Tx Rx RETRY
(dbm) db (Mbps) (Mbps) bps bps AVG

ap6562-167598:R2 B4-C7-99-CA-A1-F0 -52 50 53 36 1 k 3 k 10

```



```

Total number of radios displayed: 1
NX9500(config)#
NX9500(config)#show wireless bridge candidate-ap on ap6562-167598

Client Bridge Candidate APs:
 AP-MAC BAND CHANNEL SIGNAL(dbm) STATUS
 B4-C7-99-CA-A1-F0 5 GHz 104 -39 selected

Total number of candidates displayed: 1
NX9500(config)#
NX9500(config)#show wireless bridge certificate status on ap6562-167598
Certificate Last Updated Status: Thu Jul 23 11:41:40 2017
NX9500(config)#

```

## wwan

Displays wireless WAN status

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show wwan [configuration|status] {on <DEVICE-OR-DOMAIN-NAME>}
```

### Parameters

```
show wwan [configuration|status] {on <DEVICE-OR-DOMAIN-NAME>}
```

|                            |                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wwan                       | Displays wireless WAN configuration and status details                                                                                                                                                                                                                                                                                                                                   |
| configuration              | Displays wireless WAN configuration information                                                                                                                                                                                                                                                                                                                                          |
| status                     | Displays wireless WAN status information                                                                                                                                                                                                                                                                                                                                                 |
| on <DEVICE-OR-DOMAIN-NAME> | <p>The following keyword is common to the 'configuration' and 'status' parameters:</p> <ul style="list-style-type: none"> <li>• on &lt;DEVICE-OR-DOMAIN-NAME&gt; - Optional. Displays configuration or status details on a specified device or RF Domain</li> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; - Specify the AP, wireless controller, service platform, or RF Domain name.</li> </ul> |

### Examples

```

rfs4000-229D58(config-device-00-23-68-22-9D-58)#show wwan configuration
>>> WWAN Configuration:
+-----+
| Access Port Name : isp.cingular
| User Name : testuser
| Cryptomap : map1
+-----+
rfs4000-229D58(config-device-00-23-68-22-9D-58)#
rfs4000-229D58(config-device-00-23-68-22-9D-58)#show wwan status
>>> WWAN Status:
+-----+
| State : ACTIVE
| DNS1 : 209.183.54.151
| DNS2 : 209.183.54.151

```

```
+-----
rfs4000-229D58(config-device-00-23-68-22-9D-58)#
```

### virtual-machine

Displays the VM (virtual-machine) configuration, logs, and statistics

#### Supported in the following platforms:

- Service Platforms – NX 7510, NX 95XX

#### Syntax

```
show virtual-machine [configuration|debugging|export|statistics]
show virtual-machine [configuration|statistics] {<VM-NAME>/team-urc/team-rls/
team-vowlan} {(on <DEVICE-NAME>)}
show virtual-machine debugging {level [debug/error/info/warning]} {on <DEVICE-NAME>}
show virtual-machine export <VM-NAME> {on <DEVICE-NAME>}
show virtual-machine [configuration|statistics] {<VM-NAME>/adsp/team-cmt}
```

#### Parameters

```
show virtual-machine [configuration|statistics] {<VM-NAME>/team-urc/team-rls/
team-vowlan} {(on <DEVICE-NAME>)}
```

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| virtual-machine                             | Displays the following VM-related information: configuration or statistics                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| configuration                               | Displays detailed VM configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| statistics                                  | Displays VM statistics                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| [<VM-NAME>] team-urc[team-rls] team-vowlan] | The following keywords are common to the 'configuration' and 'statistics' parameters: <ul style="list-style-type: none"> <li>• &lt;VM-NAME&gt; – Optional. Displays VM configuration or statistics for the virtual machine identified by the &lt;VM-NAME&gt; keyword. Specify the VM name.</li> <li>• team-urc – Optional. Displays TEAM-URC (IP-PBX) VM configuration/statistics</li> <li>• team-rls – Optional. Displays TEAM-RLS (Radio Link Server) VM configuration/statistics&lt;</li> <li>• team-vowlan – Optional. Displays TEAM-VoWLAN (Voice over WLAN) VM configuration/statistics</li> </ul> |
| on <DEVICE-NAME>                            | Specifies the name of the device on which the command is executed <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the service platform.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                    |

```
show virtual-machine [configuration|statistics] {<VM-NAME>/adsp/team-cmt} {(on <DEVICE-NAME>)}
```

|                 |                                                                            |
|-----------------|----------------------------------------------------------------------------|
| virtual-machine | Displays the following VM-related information: configuration or statistics |
| configuration   | Displays detailed VM configuration                                         |
| statistics      | Displays VM statistics                                                     |

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [<VM-NAME> adsp <br>team-cmt] | The following keywords are common to the 'configuration' and 'statistics' parameters: <ul style="list-style-type: none"> <li>• VM-NAME&gt; - Optional. Displays VM configuration or statistics for the virtual machine identified by the &lt;VM-NAME&gt; keyword. Specify the VM name.</li> <li>• adsp - Optional. Displays ADSP (Air-Defense Services Platform) VM configuration/statistics</li> <li>• team-cmt - Optional. Displays TEAM-CMT VM configuration/statistics</li> </ul> |
| on <DEVICE-NAME>              | Specifies the name of the device on which the command is executed<br><DEVICE-NAME> - Specify the name of the service platform.                                                                                                                                                                                                                                                                                                                                                        |

```
show virtual-machine debugging {level[debug/error/info/warning]} {on <DEVICE-NAME>}
```

|                                       |                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| virtual-machine                       | Displays the following VM-related information: configuration or statistics                                                                                                                                                                                                                                                                                                     |
| debugging                             | Displays VM debugging logs                                                                                                                                                                                                                                                                                                                                                     |
| level [debug  error <br>info warning] | Optional. Displays VM debugging logs based on the level selected. The available options are: <ul style="list-style-type: none"> <li>• debug - Displays VM logs of level debug and above</li> <li>• error - Displays VM logs of level error</li> <li>• info - Displays VM logs of level Info and above</li> <li>• warning - Displays logs of level warning and above</li> </ul> |
| on <DEVICE-NAME>                      | Specifies the name of the device on which the command is executed <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the service platform.</li> </ul>                                                                                                                                                                                          |

```
show virtual-machine export <VM-NAME> {on <DEVICE-NAME>}
```

|                      |                                                                                                                                                                                                                                                                |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| virtual-machine      | Displays the following VM-related information: configuration or statistics                                                                                                                                                                                     |
| export               | Displays VM configuration export related information                                                                                                                                                                                                           |
| <VM-NAME>]           | Displays VM configuration export related information for the virtual machine identified by the <VM-NAME> keyword. Specify the VM name.<br>The NX 9500 and NX 9510 series service platforms will display ADSP and TEAM-CMT VM configuration export information. |
| on <DEVICE-<br>NAME> | Specifies the name of the device on which the command is executed <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; - Specify the name of the service platform.</li> </ul>                                                                          |

## Examples

```
nx9500-6C8809#show virtual-machine statistics
```

```

```

| NAME     | STATE  | VCPUS | MEM (MB) | BRIDGE-IF | IP |
|----------|--------|-------|----------|-----------|----|
| WiNG     | -      | -     | 18432    | -         | -  |
| adsp     | Halted | -     | -        | unknown   | -  |
| team-cmt | Halted | -     | -        | unknown   | -  |

```

```

```
nx9500-6C8809#
```

```
nx9500-6C8809#show virtual-machine configuration
```

```

```

| NAME     | AUTOSTART | MEMORY (MB) | VCPUS |
|----------|-----------|-------------|-------|
| WiNG     | -         | 18432       | -     |
| adsp     | ignore    | 12000       | 12    |
| team-cmt | ignore    | 1024        | 1     |

```

```

---

```
nx9500-6C8809#
nx9500-6C8809>show virtual-machine statistics adsp
 VM name: adsp
 Base Version : unknown
 Install Status : not_installed
nx9500-6C8809>
```

# PROFILE COMMANDS

## PROFILES

---

Profiles enable administrators to assign a common set of configuration parameters, policies, and WLANs to service platforms, controllers, and access points across a large, multi segment, site. The configuration parameters within a profile are based on the hardware model the profile was created to support.

The service platforms, wireless controllers, and access points support both default and user-defined profiles. Each default and user-defined profile contains policies and configurations that are applied to devices assigned to the profile. Changes made to these configurations are automatically inherited by the devices. The central benefit of a profile is its ability to update devices collectively without having to modify individual device configurations.

Default profiles are system maintained and are automatically applied to service platforms and wireless controllers. The default AP profile is automatically applied to a AP (discovered by a wireless controller or service platform), unless an AP auto-provisioning policy is defined specifically to assign APs to a user-defined profile. After adoption, changes made to a profile's parameters are reflected across all devices using the profile. Default profiles are ideal for single site deployments where service platforms, wireless controllers, and access points share a common configuration.

User-defined profiles, on the other hand, are manually created for each supported service platform, wireless controller, and access point model. User-defined profiles are recommended for larger deployments using centralized controllers and service platforms when groups of devices on different floors, buildings or sites share a common configuration. These user-defined profiles can be manually, or automatically assigned to through an auto provisioning policy. An auto provisioning policy provides the means to assign profiles to access points based on model, serial number, VLAN ID, DHCP options, IP address (subnet) and MAC address. For more information, see [AUTO-PROVISIONING-POLICY](#) on page 1336.

A user-defined profile can be created for each of the following device type:

- AP 6522 – Adds an AP 6522 access point profile
- AP 6562 – Adds an AP 6562 access point profile
- AP 7161 – Adds an AP 7161 access point profile
- AP 7502 – Adds an AP 7502 access point profile
- AP 7522 – Adds an AP 7522 access point profile
- AP 7532 – Adds an AP 7532 access point profile
- AP 7562 – Adds an AP 7562 access point profile
- AP 7602 – Adds an AP 7602 access point profile
- AP 7612 – Adds an AP 7612 access point profile
- AP 7622 – Adds an AP 7622 access point profile
- AP 7632 – Adds an AP 7632 access point profile
- AP 7662 – Adds an AP 7662 access point profile
- AP 8163 – Adds an AP 8163 access point profile

- AP 8432 – Adds an AP 8432 access point profile
- AP 8533 – Adds an AP 8533 access point profile
- EX3524 – Adds an EX3524 wireless controller profile
- EX3548 – Adds an EX3548 wireless controller profile
- RFS 4000 – Adds an RFS 4000 wireless controller profile
- NX 5500 – Adds an NX 5500 wireless controller profile
- NX 7500 – Adds an NX 75XX series service platform profile
- NX 9000 – Adds an NX 95XX series service platform profile
- NX 9600 – Adds an NX 96XX series service platform profile
- VX 9000 – Adds a VX 9000 virtual controller profile
- T5 – Adds a T5 controller profile



**Note**

A T5 profile can be created only on the following platforms: RFS 4000, NX 95XX, and NX 96XX.

Although profiles assign a common set of configuration parameters across devices, individual devices can still be assigned unique configuration parameters that follow the flat configuration model. As individual device updates are made, these devices no longer share the profile based configuration they originally supported. Therefore, changes made to a profile are not automatically inherited by devices who have had their configuration customized. These devices require careful administration, as they cannot be tracked as profile members. Their customized configurations overwrite their profile configurations until the profile is re-applied.



**Note**

The commands present under ‘Profiles’ are also available under the ‘Device mode’. The additional commands specific to the ‘Device mode’ are listed separately.

This chapter is organized into the following topics:

- [Profile Config Commands](#) on page 862
- [Device Config Commands](#) on page 1252
- [T5 Profile Config Commands](#) on page 1285
- [EX3524 & EX3548 Profile/Device Config Commands](#) on page 1296

To view the list of device profiles supported, use the following command:

```
<DEVICE>(config)#profile ?
nx9500-6C8809(config)#profile ?
anyap Any access point profile
ap621 AP621 access point profile
ap622 AP622 access point profile
ap650 AP650 access point profile
ap6511 AP6511 access point profile
ap6521 AP6521 access point profile
ap6522 AP6522 access point profile
ap6532 AP6532 access point profile
ap6562 AP6562 access point profile
ap71xx AP71XX access point profile
ap7502 AP7502 access point profile
ap7522 AP7522 access point profile
ap7532 AP7532 access point profile
```

```

ap7562 AP7562 access point profile
ap7602 AP7602 access point profile
ap7612 AP7612 access point profile
ap7622 AP7622 access point profile
ap7632 AP7632 access point profile
ap7662 AP7662 access point profile
ap81xx AP81XX access point profile
ap82xx AP82XX access point profile
ap8432 AP8432 access point profile
ap8533 AP8533 access point profile
containing Specify profiles that contain a sub-string in the profile name
ex3524 EX3524 wireless controller profile
ex3548 EX3548 wireless controller profile
filter Specify addition selection filter
nx45xx NX45XX integrated services platform profile
nx5500 NX5500 wireless controller profile
nx65xx NX65XX integrated services platform profile
nx75xx NX75XX wireless controller profile
nx9000 NX9000 wireless controller profile
rfs4000 RFS4000 wireless controller profile
rfs6000 RFS6000 wireless controller profile
rfs7000 RFS7000 wireless controller profile
t5 T5 DSL switch profile
vx9000 VX9000 wireless controller profile
<cr>

```

```
nx9500-6C8809(config)#
```

```
nx9500-6C8809(config)#profile nx9000 default-nx9000
nx9500-6C8809(config-profile-default-nx9000)#
```

```
nx9500-6C8809(config)#profile ap8432 default-ap8432
nx9500-6C8809(config-profile-default-ap8432)#
```

```
<DEVICE>(config)#profile <DEVICE-TYPE> <PROFILE-NAME>
<DEVICE>(config-profile-<PROFILE-NAME>)#
```

```
nx9500-6C8809(config-profile-default-nx9000)#?
```

```
Profile Mode commands:
```

```

adopter-auto-provisioning-policy-lookup Use centralized auto-provisioning
 policy when adopted by another
 controller
adoption Adoption configuration
adoption-mode Configure the adoption mode for the
 access-points in this RF-Domain
alias Alias
application-policy Application Policy configuration
area Set name of area where the system
 is located
arp Address Resolution Protocol (ARP)
auto-learn Auto learning
autogen-uniqueid Autogenerate a unique id
autoinstall Autoinstall settings
bridge Ethernet bridge
captive-portal Captive portal
cdp Cisco Discovery Protocol
cluster Cluster configuration
configuration-persistence Enable persistence of configuration
 across reloads (startup config
 file)
controller WLAN controller configuration
critical-resource Critical Resource
crypto Encryption related commands
database Database command

```

|                                    |                                                                                 |
|------------------------------------|---------------------------------------------------------------------------------|
| device-onboard                     | Device-onboarding configuration                                                 |
| device-upgrade                     | Device firmware upgrade                                                         |
| diag                               | Diagnosis of packets                                                            |
| dot1x                              | 802.1X                                                                          |
| dpi                                | Enable Deep-Packet-Inspection (Application Assurance)                           |
| dscp-mapping                       | Configure IP DSCP to 802.1p priority mapping for untagged frames                |
| eguest-server                      | Configure ExtremeGuest server                                                   |
| email-notification                 | Email notification configuration                                                |
| enforce-version                    | Check the firmware versions of devices before interoperating                    |
| environmental-sensor               | Environmental Sensors Configuration                                             |
| events                             | System event messages                                                           |
| export                             | Export a file                                                                   |
| file-sync                          | File sync between controller and adoptees                                       |
| floor                              | Set the floor within a area where the system is located                         |
| gre                                | GRE protocol                                                                    |
| http-analyze                       | Specify HTTP-Analysis configuration                                             |
| interface                          | Select an interface to configure                                                |
| ip                                 | Internet Protocol (IP)                                                          |
| ipv6                               | Internet Protocol version 6 (IPv6)                                              |
| l2tpv3                             | L2tpv3 protocol                                                                 |
| l3e-lite-table                     | L3e lite Table                                                                  |
| led                                | Turn LEDs on/off on the device                                                  |
| led-timeout                        | Configure the time for the led to turn off after the last radio state change    |
| legacy-auto-downgrade              | Enable device firmware to auto downgrade when other legacy devices are detected |
| legacy-auto-update                 | Auto upgrade of legacy devices                                                  |
| lldp                               | Link Layer Discovery Protocol                                                   |
| load-balancing                     | Configure load balancing parameter                                              |
| logging                            | Modify message logging facilities                                               |
| mac-address-table                  | MAC Address Table                                                               |
| mac-auth                           | 802.1X                                                                          |
| management-server                  | Configure management server address                                             |
| memory-profile                     | Memory profile to be used on the device                                         |
| meshpoint-device                   | Configure meshpoint device parameters                                           |
| meshpoint-monitor-interval         | Configure meshpoint monitoring interval                                         |
| min-misconfiguration-recovery-time | Time interval to check controller connectivity after configuration is received  |
| mint                               | MiNT protocol                                                                   |
| misconfiguration-recovery-time     | Check controller connectivity after configuration is received                   |
| neighbor-inactivity-timeout        | Configure neighbor inactivity timeout                                           |
| neighbor-info-interval             | Configure neighbor information exchange interval                                |
| no                                 | Negate a command or set its defaults                                            |
| noc                                | Configure the noc related setting                                               |
| nsight                             | NSight                                                                          |
| ntp                                | Ntp server WORD                                                                 |
| offline-duration                   | Set duration for which a device remains unadopted before it                     |



|                             |                                                                                    |
|-----------------------------|------------------------------------------------------------------------------------|
| otls                        | generates offline event                                                            |
| power-config                | Omnitrail Location Server                                                          |
| preferred-controller-group  | Configure power mode                                                               |
|                             | Controller group this system will prefer for adoption                              |
| preferred-tunnel-controller | Tunnel Controller Name this system will prefer for tunneling extended vlan traffic |
| radius                      | Configure device-level radius authentication parameters                            |
| raid                        | RAID                                                                               |
| remote-debug                | Configure remote debug parameters                                                  |
| remove-override             | Remove configuration item override from the device (so profile value takes effect) |
| rf-domain-manager           | RF Domain Manager                                                                  |
| router                      | Dynamic routing                                                                    |
| slot                        | PCI expansion Slot                                                                 |
| spanning-tree               | Spanning tree                                                                      |
| traffic-class-mapping       | Configure IPv6 traffic class to 802.1p priority mapping for untagged frames        |
| traffic-shape               | Traffic shaping                                                                    |
| trustpoint                  | Assign a trustpoint to a service                                                   |
| tunnel-controller           | Tunnel Controller group this controller belongs to                                 |
| use                         | Set setting to use                                                                 |
| vrrp                        | VRRP configuration                                                                 |
| vrrp-state-check            | Publish interface via OSPF/BGP only if the interface VRRP state is not BACKUP      |
| wep-shared-key-auth         | Enable support for 802.11 WEP shared key authentication                            |
| zone                        | Configure Zone name                                                                |
| clrscr                      | Clears the display screen                                                          |
| commit                      | Commit all changes made in this session                                            |
| do                          | Run commands from Exec mode                                                        |
| end                         | End current mode and change to EXEC mode                                           |
| exit                        | End current mode and down to previous mode                                         |
| help                        | Description of the interactive help system                                         |
| revert                      | Revert changes                                                                     |
| service                     | Service Commands                                                                   |
| show                        | Show running system information                                                    |
| write                       | Write running configuration to memory or terminal                                  |

nx9500-6C8809(config-profile-default-nx9000)#

nx9500-6C8809(config-profile-T5Profile)#?

T5 Profile Mode commands:

|               |                                              |
|---------------|----------------------------------------------|
| cpe           | T5 CPE configuration                         |
| interface     | Select an interface to configure             |
| ip            | Internet Protocol (IP)                       |
| no            | Negate a command or set its defaults         |
| ntp           | Configure NTP                                |
| override-wlan | Configure RF Domain level overrides for wlan |
| t5            | T5 configuration                             |
| t5-logging    | Modify message logging facilities            |
| use           | Set setting to use                           |

```

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

```

```
nx9500-6C8809(config-profile-T5Profile)#
```

```
nx9500-6C8809(config-profile-Ex3524Profile)#?
```

```
EX35xx Profile Mode commands:
```

```

interface Select an interface to configure
ip Internet Protocol (IP)
no Negate a command or set its defaults
power Ex3500 Power over Ethernet Command
upgrade Configures upgrade option for ex3500 system
use Set setting to use

```

```

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

```

```
nx9500-6C8809(config-profile-Ex3524Profile)#
```



### Note

The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (\_) character. In other words, the name of a device cannot contain an underscore.

## Profile Config Commands

The following table summarizes profile configuration mode commands:

**Table 33: Profiles Config Mode Commands**

| Command                                                             | Description                                                                                                                                          |
|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">adopter-auto-provisioning-policy-lookup</a> on page 866 | Enables the use of a centralized auto provisioning policy on this profile                                                                            |
| <a href="#">adoption</a> on page 867                                | Configures a minimum and maximum delay time in the initiation of the device adoption process                                                         |
| <a href="#">adoption-mode</a> on page 868                           | Sets the adoption mode for access points to Controller, clou, or Extreme Services                                                                    |
| <a href="#">alias</a> on page 870                                   | Creates various types of aliases, such as network, VLAN, network-group, network-service, encrypted-string, hashed -string, etc. at the profile level |

**Table 33: Profiles Config Mode Commands (continued)**

| Command                                                 | Description                                                                                                                                                                                                             |
|---------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">application-policy</a> on page 878          | Associates a RADIUS server provided application policy with this profile. When associated, the application policy allows wireless clients (MUs) to always find the RADIUS-supplied application policy in the dataplane. |
| <a href="#">area</a> on page 879                        | Sets the system's area of location (the area name)                                                                                                                                                                      |
| <a href="#">arp</a> on page 880                         | Configures static address resolution protocol                                                                                                                                                                           |
| <a href="#">auto-learn</a> on page 882                  | Enables controllers or service platforms to maintain a local configuration record of devices requesting adoption and provisioning. The command also enables learning of a device's host name via DHCP options.          |
| <a href="#">autogen-uniqueid</a> on page 883            | Auto-generates a unique local ID for devices using this profile. When executed in the device configuration mode, this command generates a unique ID for the logged device.                                              |
| <a href="#">autoinstall</a> on page 884                 | Configures the automatic install feature                                                                                                                                                                                |
| <a href="#">bridge</a> on page 885                      | Configures bridge specific parameters                                                                                                                                                                                   |
| <a href="#">captive-portal</a> on page 913              | Configures captive portal advanced Web page upload on a device profile                                                                                                                                                  |
| <a href="#">cdp</a> on page 914                         | Enables Cisco Discovery Protocol (CDP) on a device                                                                                                                                                                      |
| <a href="#">cluster</a> on page 915                     | Configures a cluster name                                                                                                                                                                                               |
| <a href="#">configuration-persistence</a> on page 917   | Enables persistence of configuration across reloads                                                                                                                                                                     |
| <a href="#">controller</a> on page 918                  | Configures a wireless controller or service platform                                                                                                                                                                    |
| <a href="#">critical-resource</a> on page 923           | Monitors resources that are critical to the health of the service platform, wireless controller, or access point managed network. These critical resources are identified by their configured IP addresses.             |
| <a href="#">crypto</a> on page 931                      | Configures data encryption related protocols and settings                                                                                                                                                               |
| <a href="#">database</a> on page 979                    | Backs up captive-portal and/or NSight database to a specified location and file and configures a low-disk-space threshold value                                                                                         |
| <a href="#">device-onboard</a> on page 980              | Configures the logo image file name and title displayed on the EGuest device-onboarding portal. This is the portal a vendor-admin user uses to onboard devices.                                                         |
| <a href="#">device-upgrade</a> on page 981              | Configures device firmware upgrade settings on this profile                                                                                                                                                             |
| <a href="#">diag</a> on page 983                        | Enables looped packet logging                                                                                                                                                                                           |
| <a href="#">dot1x</a> on page 984                       | Configures 802.1x standard authentication controls                                                                                                                                                                      |
| <a href="#">dpi</a> on page 986                         | Enables DPI (Deep Packet Inspection) on this profile                                                                                                                                                                    |
| <a href="#">dscp-mapping</a> on page 989                | Configures an IP DSCP to 802.1p priority mapping for untagged frames                                                                                                                                                    |
| <a href="#">eguest-server (VX9000 only)</a> on page 990 | Enables the EGuest daemon when executed without the 'host' option                                                                                                                                                       |

**Table 33: Profiles Config Mode Commands (continued)**

| Command                                              | Description                                                                                                                                      |
|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">eguest-server (NOC Only)</a> on page 991 | Points to the EGuest server, when executed along with the 'host' option                                                                          |
| <a href="#">email-notification</a> on page 992       | Configures e-mail notification settings                                                                                                          |
| <a href="#">enforce-version</a> on page 994          | Enables checking of a device's firmware version before attempting adoption or clustering                                                         |
| <a href="#">environmental-sensor</a> on page 995     | Configures the environmental sensor settings on this profile (applicable to AP8132 model access point only)                                      |
| <a href="#">events</a> on page 998                   | Enables system event logging and message generation. This command also configures event message forwarding settings.                             |
| <a href="#">export</a> on page 998                   | Enables export of startup.log file after every boot                                                                                              |
| <a href="#">file-sync</a> on page 999                | Configures parameters enabling synching of trustpoint and/or wireless-bridge certificate between the staging-controller and adopted access point |
| <a href="#">floor</a> on page 1000                   | Sets the floor name where the system is located                                                                                                  |
| <a href="#">gre</a> on page 1001                     | Enables Generic Routing Encapsulation (GRE) tunneling on this profile                                                                            |
| <a href="#">http-analyze</a> on page 1011            | Configures HTTP analysis settings                                                                                                                |
| <a href="#">interface</a> on page 1013               | Configures an interface (VLAN, radio, GE, etc.)                                                                                                  |
| <a href="#">ip</a> on page 1154                      | Configures IPv4 components                                                                                                                       |
| <a href="#">ipv6</a> on page 1162                    | Configures IPv6 components                                                                                                                       |
| <a href="#">l2tpv3</a> on page 1167                  | Defines the L2TP (Layer 2 Tunnel Protocol) for tunneling layer 2 payloads using VPNs (Virtual Private Networks)                                  |
| <a href="#">l3e-lite-table</a> on page 1169          | Configures L3e Lite Table with this profile                                                                                                      |
| <a href="#">led</a> on page 1169                     | Turns device LEDs on or off                                                                                                                      |
| <a href="#">led-timeout</a> on page 1170             | Configures LED-timeout timer. This command is specific to the NX 95XX series service platforms.                                                  |
| <a href="#">legacy-auto-downgrade</a> on page 1171   | Auto downgrades a legacy device firmware                                                                                                         |
| <a href="#">legacy-auto-update</a> on page 1172      | Auto upgrades a legacy device firmware                                                                                                           |
| <a href="#">lldp</a> on page 1173                    | Configures LLDP (Link Layer Discovery Protocol) settings                                                                                         |
| <a href="#">load-balancing</a> on page 1174          | Configures load balancing parameters                                                                                                             |
| <a href="#">logging</a> on page 1180                 | Modifies message logging settings                                                                                                                |
| <a href="#">mac-address-table</a> on page 1182       | Configures the MAC address table                                                                                                                 |
| <a href="#">mac-auth</a> on page 1183                | Enables 802.1x user authentication protocol on this profile                                                                                      |

**Table 33: Profiles Config Mode Commands (continued)**

| Command                                                         | Description                                                                                                                                                                          |
|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">management-server</a> on page 1186                  | Configures a management server with this profile                                                                                                                                     |
| <a href="#">meshpoint-device</a> on page 1187                   | Configures a meshpoint device parameters                                                                                                                                             |
| <a href="#">meshpoint-monitor-interval</a> on page 1188         | Configures meshpoint monitoring interval                                                                                                                                             |
| <a href="#">min-misconfiguration-recovery-time</a> on page 1189 | Configures the minimum device connectivity verification time                                                                                                                         |
| <a href="#">mint</a> on page 1190                               | Configures MiNT protocol settings                                                                                                                                                    |
| <a href="#">misconfiguration-recovery-time</a> on page 1197     | Verifies device connectivity after a configuration is received                                                                                                                       |
| <a href="#">neighbor-inactivity-timeout</a> on page 1198        | Configures neighbor inactivity timeout                                                                                                                                               |
| <a href="#">neighbor-info-interval</a> on page 1199             | Configures neighbor information exchange interval                                                                                                                                    |
| <a href="#">no</a> on page 1200                                 | Removes or reverts settings to their default. The no command, when used in the profile configuration mode, removes the selected profile's settings or reverts them to their default. |
| <a href="#">noc</a> on page 1202                                | Configures NOC settings                                                                                                                                                              |
| <a href="#">nsight</a> on page 1202                             | Configures NSight database related parameters                                                                                                                                        |
| <a href="#">ntp</a> on page 1207                                | Configures NTP server settings                                                                                                                                                       |
| <a href="#">otls</a> on page 1210                               | Configures support for detection and forwarding of OmniTrail beacon tags                                                                                                             |
| <a href="#">offline-duration</a> on page 1212                   | Sets the duration, in minutes, for which a device remains un-adopted before it generates offline event                                                                               |
| <a href="#">power-config</a> on page 1213                       | Configures the power mode                                                                                                                                                            |
| <a href="#">preferred-controller-group</a> on page 1215         | Specifies the wireless controller or service platform group preferred for adoption                                                                                                   |
| <a href="#">preferred-tunnel-controller</a> on page 1215        | Configures the tunnel wireless controller or service platform preferred by the system to tunnel extended VLAN traffic                                                                |
| <a href="#">radius</a> on page 1216                             | Configures device-level RADIUS authentication parameters                                                                                                                             |
| <a href="#">raid</a> on page 1284                               | Enables alarm on the array. This command is supported only on the NX 95XX series service platform profile/device config modes.                                                       |
| <a href="#">rf-domain-manager</a> on page 1217                  | Enables devices using this profile to be elected as RF Domain manager. Also sets the priority value for devices using this profile in the RF Domain manager election process.        |
| <a href="#">router</a> on page 1218                             | Configures dynamic router protocol settings                                                                                                                                          |
| <a href="#">spanning-tree</a> on page 1220                      | Configures spanning tree related settings                                                                                                                                            |

**Table 33: Profiles Config Mode Commands (continued)**

| Command                                                       | Description                                                                                                                                                             |
|---------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">traffic-class-mapping</a> on page 1223            | Maps the IPv6 traffic class value of incoming IPv6 untagged packets to 802.1p priority                                                                                  |
| <a href="#">traffic-shape</a> on page 1224                    | Enables traffic shaping and configures traffic shaping parameters                                                                                                       |
| <a href="#">trustpoint (profile-config-mode)</a> on page 1229 | Configures the trustpoint assigned for validating a CMP auth Operator                                                                                                   |
| <a href="#">tunnel-controller</a> on page 1231                | Configures the name of tunneled WLAN (extended VLAN) wireless controller or service platform                                                                            |
| <a href="#">use</a> on page 1232                              | Uses pre configured policies with this profile                                                                                                                          |
| <a href="#">vrrp</a> on page 1238                             | Configures VRRP (Virtual Router Redundancy Protocol) group settings                                                                                                     |
| <a href="#">vrrp-state-check</a> on page 1242                 | Publishes interface via OSPF or BGP based on VRRP status                                                                                                                |
| <a href="#">virtual-controller</a> on page 1243               | Enables an access point as a VC (virtual-controller) or DVC (dynamic virtual controller). Note, DVC is supported only on the AP 7522, AP 7532, and model access points. |
| <a href="#">wep-shared-key-auth</a> on page 1244              | Enables support for 802.11 WEP shared key authentication                                                                                                                |
| <a href="#">service</a> on page 1245                          | Service commands are used to view and manage configurations. The service commands and their corresponding parameters vary from mode to mode.                            |
| <a href="#">zone</a> on page 1251                             | Configures the zone for devices using this profile. The zone can also be configured on the device's self context.                                                       |

**Note**

For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see [COMMON COMMANDS](#) on page 640.

**Note**

The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (\_) character. In other words, the name of a device cannot contain an underscore.

*adopter-auto-provisioning-policy-lookup*

[Profile Config Commands](#) on page 862

Enables the use of a centralized auto provisioning policy on this profile. When enabled, the auto-provisioning policy applied on the NOC gets precedence over the one applied at the site controller level. Optionally, use the 'evaluate-always' option to set flag to run centralized auto-provisioning policy every time a device (access point/controller) is adopted. The device's previous adoption status is not taken into consideration.

This command is also applicable in the device configuration context.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
adopter-auto-provisioning-policy-lookup {evaluate-always}
```

### Parameters

```
adopter-auto-provisioning-policy-lookup {evaluate-always}
```

|                                                           |                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| adopter-auto-provisioning-policy-lookup {evaluate-always} | Enables the use of a centralized auto provisioning policy on this profile or device <ul style="list-style-type: none"><li>• evaluate-always - Optional. Sets flag to run centralized auto-provisioning policy every time a device (access point/controller) is adopted.</li></ul> |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
nx9500-6C8809(config-profile-test4K)#adopter-auto-provisioning-policy-lookup
evaluate-always
nx9500-6C8809(config-profile-test4K)#show context include-factory | include adopter-auto-
provisioning-policy-lookup
 adopter-auto-provisioning-policy-lookup evaluate-always
nx9500-6C8809(config-profile-test4K)#
```

### Related Commands

|    |              |                                                                                            |
|----|--------------|--------------------------------------------------------------------------------------------|
| no | on page 1200 | Disables the application of centralized auto provisioning policy on this profile or device |
|----|--------------|--------------------------------------------------------------------------------------------|

## adoption

[Profile Config Commands](#) on page 862

Configures a minimum and maximum delay time in the initiation of the device adoption process. When configured, devices do not attempt adoption immediately on coming up. The process is initiated after the lapse of a specified period of time (configured using this command as the start-delay minimum time).

Once configured and applied, this setting is applicable on all devices using this profile. This option is also available in the device-configuration mode.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
adoption start-delay min <0-30> max <0-30>
```

## Parameters

`adoption start-delay min <0-30> max <0-30>`

|                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>adoption start-delay min &lt;0-30&gt; max &lt;0-30&gt;</code> | <p>Delays start of the device adoption process</p> <ul style="list-style-type: none"><li>• <code>min &lt;0-30&gt;</code> - Configures the minimum time to lapse before a device attempts adoption. Specify a value from 0 - 30 seconds.</li></ul> <p>A device, on coming up, attempts adoption only after the lapse of the time specified here. The default is 5 seconds.</p> <ul style="list-style-type: none"><li>• <code>max &lt;0-30&gt;</code> - Configures the maximum time to lapse before a device attempts adoption. Specify a value from 0 - 30 seconds. The default is 20 seconds.</li></ul> |
|---------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
nx9500-6C8809(config-profile-test4K)#adoption start-delay min 10 max 30
nx9500-6C8809(config-profile-test4K)#show context include-factory | include adoption
enforce-version adoption strict
controller adoption
adoption start-delay min 10 max 30
adoption-mode controller
nx9500-6C8809(config-profile-test4K)#
```

## Related Commands

|                              |                                                                                                                    |
|------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <code>no</code> on page 1200 | Removes the configured minimum start-delay value. When removed, devices attempt adoption immediately on coming up. |
|------------------------------|--------------------------------------------------------------------------------------------------------------------|

### *adoption-mode*

[Profile Config Commands](#) on page 862

Configures the mode of adoption in an access point profile. This command is also applicable to the device configuration context.

By default, any WiNG AP, on being powered-up for the first time, starts the following auto-discovery process. The AP:

- 1 Moves to MLCP\_DISCOVERY state and tries to discover a local controller. If a local controller is found, it
  - a adopts to the controller, and
  - b marks itself as “local-controller” adopted, and
  - c moves to the MLCP\_MODE.
- 2 If a local controller is not found, the AP switches to the CLOUD\_DISCOVERY state, and tries connecting to the ExtremeCloud. If the AP succeeds in connecting to the cloud, it
  - a marks itself as “cloud-adopted”, and
  - b moves to the CLOUD\_MODE.
- 3 If the AP is unable to discover and adopt to the ExtremeCloud, it switches to the WS\_CONTROLLER\_DISCOVERY state, and tries connecting to the WebSocket (WS) Controller. If it succeeds in connecting to the ws\_controller, it
  - a marks itself as “ws-controller-adopted”, and
  - b moves to the WS\_CONTROLLER\_MODE.



- 4 The AP continues to switch between the three discovery states (local controller, cloud, and ws\_controller) until it gets adopted.
- 5 Once adopted, an AP's adoption mode does not change unless,
  - a It is changed from the controller's CLI (using the adoption-mode command), the Cloud dashboard, or the WS controller dashboard.
  - b If the AP is reverted to factory settings, in which case the AP starts the auto-discovery process on bootup.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

adoption-mode [cloud|controller|ws-controller]

### Parameters

adoption-mode [cloud|controller|ws-controller]

|                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>adoption-mode<br/>[cloud controller ws-controller]</p> | <p>Use to set the adoption-mode to:</p> <ul style="list-style-type: none"> <li>• cloud - Sets the adoption-mode to Extreme Cloud. The factory-default, management server setting, in WiNG AP profiles contexts, points to the Extreme Cloud Web address. If the adoption-mode is set to cloud, the AP on coming up, will search for and adopt to the ExtremeCloud.</li> <li>• controller - Sets the adoption mode to the local WiNG controller. This is the default setting. Note, APs with the 'controller &gt; host &gt; configuration' specified are marked as local-controller APs and never try adopting to the CLOUD or WS-Controller</li> <li>• ws-controller - Sets the adoption mode to the EAE (Edge Application Engine) ws-controller. If selecting this option, use the 'management-server' command to configure the EAE controller's IP address or hostname. For information on configuring the management-server, see <a href="#">management-server</a> on page 1186.</li> </ul> <p><b>Note:</b> Alternately, the AP auto-adopts to the WS controller, if its receives DHCP IP address, and the DHCP option 191 pool string configuration is as shown in the following examples:</p> <p>In the DHCP server policy, define an alias for option 191:</p> <pre>VX(config-dhcp-policy-DHCP)#   dhcp-server-policy DHCP     option AP-adoption 191 ascii</pre> <p>In the DHCP pool config, define the option 191 string:</p> <pre>dhcp-pool AP   option AP-adoption pool1=&lt;ws-controller-ip-address&gt;;   adoption-mode=ws-controller</pre> |
|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
nx9500-6C8809(config-profile-testAP8432)#adoption-mode cloud
nx9500-6C8809(config-profile-testAP8432)#show context
profile ap8432 testAP8432
 no autoinstall configuration
 no autoinstall firmware
 crypto ikev1 policy ikev1-default
```

```

isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ikev2 policy ikev2-default
isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
crypto ikev1 remote-vpn
crypto ikev2 remote-vpn
crypto auto-ipsec-secure
crypto load-management
crypto remote-vpn-client
interface radiol
interface radio2
interface bluetooth1
shutdown
interface ge1
interface ge2
interface pppoe1
use firewall-policy default
service pm sys-restart
router ospf
adoption-mode cloud
nx9500-6C8809(config-profile-testAP8432)#
ap8432-070235(config-device-74-67-F7-07-02-35)#adoption-mode ws-controller
ap8432-070235(config-device-74-67-F7-07-02-35)#show context
ap8432 74-67-F7-07-02-35
use profile default-ap8432
use rf-domain default
hostname ap8432-070235
ip default-gateway 10.234.160.254
ip route 10.233.84.0/24 10.234.160.254
use radius-server-policy cb-tp
interface radio2
interface ge1
switchport mode access
switchport access vlan 1
interface vlan1
ip address 10.234.160.13/24
adoption-mode ws-controller
ap8432-070235(config-device-74-67-F7-07-02-35)#

```

## Related Commands

|                              |                                                   |
|------------------------------|---------------------------------------------------|
| <code>no</code> on page 1200 | Reverts the adoption-mode to default (controller) |
|------------------------------|---------------------------------------------------|

*alias*

[Profile Config Commands](#) on page 862

Configures network, VLAN, and service aliases. The aliases defined on this profile applies to all devices using this profile. Aliases can be also defined at the device level.



### Note

You can apply overrides to aliases at the device level. Overrides applied at the device level take precedence. For more information on aliases, see [alias](#) on page 237 (global config mode).

## Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000

- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
alias [address-range|encrypted-string|hashed-string|host|network|network-group|
network-service|number|string|vlan]
alias address-range <ADDRESS-RANGE-ALIAS-NAME> <STARTING-IP> to <ENDING-IP>
alias encrypted-string <ENCRYPTED-STRING-ALIAS-NAME> <LINE>
alias hashed-string <HASHED-STRING-ALIAS-NAME> <LINE>
alias host <HOST-ALIAS-NAME> <HOST-IP>
alias network <NETWORK-ALIAS-NAME> <NETWORK-ADDRESS/MASK>
alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range|host|network]
alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range <STARTING-IP> to <ENDING-IP>|
host <HOST-IP>|network <NETWORK-ADDRESS/MASK>]
alias network-service <NETWORK-SERVICE-ALIAS-NAME> proto [<0-254>|<WORD>|eigrp| gre|igmp|
igmp|
ospf|vrrp] {(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher|https| ldap|nntp|ntp|pop3|proto|
sip|smtp|
sourceport|ssh|telnet|tftp|www)}
```

### Parameters

```
alias address-range <ADDRESS-RANGE-ALIAS-NAME> <STARTING-IP> to <ENDING-IP>
```

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| address-range<br><ADDRESS-RANGE-ALIAS-NAME> | Creates a new address-range alias for this profile. Or associates an existing address-range alias with this profile. An address-range alias maps a name to a range of IP addresses. Use this option to create unique address-range aliases for different deployment scenarios.                                                                                                                                                                                                                                                                                                                                              |
|                                             | <p>For example, if an ACL defines a pool of network addresses as 192.168.10.10 through 192.168.10.100 for an entire network, and a remote location's network range is 172.16.13.20 through 172.16.13.110, the remote location's ACL can be overridden using an alias. At the remote location, the ACL works with the 172.16.13.20-110 address range. A new ACL need not be created specifically for the remote deployment location.</p> <ul style="list-style-type: none"> <li>• &lt;ADDRESS-RANGE-ALIAS-NAME&gt; - Specify the address range alias name.</li> </ul> <p><b>Note:</b> Alias name should begin with '\$'.</p> |
| <STARTING-IP> to<br><ENDING-IP>             | <p>Associates a range of IP addresses with this address range alias</p> <ul style="list-style-type: none"> <li>• &lt;STARTING-IP&gt; - Specify the first IP address in the range.</li> <li>• to &lt;ENDING-IP&gt; - Specify the last IP address in the range.</li> </ul> <p>Aliases defined at any given level can be overridden at the next lower levels. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence.</p>                                                                                                   |

```
alias encrypted-string <ENCRYPTED-STRING-ALIAS-NAME> <LINE>
```

|                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>encrypted-string</b><br><b>&lt;ENCRYPTED-STRING-ALIAS-NAME&gt;</b> | <p>Creates an alias for an encrypted string. Use this alias for string configuration values that are encrypted when "password-encryption" is enabled. For example, in the management-policy, use it to define the SNMP community string. For more information, see <a href="#">snmp-server</a> on page 1537 (management policy config mode).</p> <ul style="list-style-type: none"> <li>• &lt;ENCRYPTED-STRING-ALIAS-NAME&gt; - Specify the encrypted-string alias name.</li> </ul> <p>Alias name should begin with '\$'.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>&lt;LINE&gt;</b>                                                   | <p>Configures the value associated with the alias name specified in the previous step</p> <ul style="list-style-type: none"> <li>• &lt;LINE&gt; - Configures the alias value</li> </ul> <p><b>Note:</b> If password-encryption is enabled, in the <b>show &gt; running-config</b> output, this clear text is displayed as an encrypted string, as shown below:</p> <pre data-bbox="527 604 1425 787"> nx9500-6C8809(config)#show running-config !..... alias encrypted-string \$enString 2 fABMK2is7UToNiZE3MQXbgAAAxB0ZIysdqseJwr6AH/Da// ! --More-- nx9500-6C8809 </pre> <p>In the above output, the '2' displayed before the encrypted-string alias value indicates that the displayed text is encrypted and not a clear text. However, if password-encryption is disabled the clear text is displayed as is:</p> <pre data-bbox="527 949 1425 1131"> nx9500-6C8809(config)#show running-config !..... ! alias encrypted-string \$enString 0 test11223344 ! --More-- nx9500-6C8809 </pre> <p>For more information on enabling password-encryption, see <a href="#">password-encryption</a> on page 487.</p> |

alias hashed-string <HASHED-STRING-ALIAS-NAME> <LINE>



|                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>hashed-string</b><br><b>&lt;HASHED-STRING-ALIAS-NAME&gt;</b> | <p>Creates an alias for a hashed string. Use this alias for configuration values that are hashed strings, such as passwords. For example, in the management-policy, use it to define the privilege mode password. For more information, see <a href="#">privilege-mode-password</a> on page 1532 (management-policy mode).</p> <ul style="list-style-type: none"> <li>• &lt;HASHED-STRING-ALIAS-NAME&gt; - Specify the hashed-string alias name.</li> </ul> <p>Alias name should begin with '\$'.</p>                                |
| <b>&lt;LINE&gt;</b>                                             | <p>Configures the hashed-string value associated with this alias.</p> <pre> nx9500-6C8809(config)#show running-config ! alias encrypted-string \$WRITE 2 sBqVCDAoxs3oByF5PCSuFAAAAAd7HT2+EiT/1/ BXm9c4SBDv ! alias hashed-string \$PriMode 1 faffdde27cb49ad634ea20df4f7c8ef2685894d10ffcb1b2efba054112ecfc75 --More-- nx9500-6C8809 </pre> <p>In the above <code>show &gt; running-config</code> output, the '!' displayed before the hashed-string alias value indicates that the displayed text is hashed and not clear text.</p> |

```
alias host <HOST-ALIAS-NAME> <HOST-IP>
```

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>host &lt;HOST-ALIAS-NAME&gt;</b> | <p>Creates a new host alias for this profile. Or associates an existing host alias with this profile. A host alias configuration is for a particular host device's IP address. Use this option to create unique host aliases for different deployment scenarios. For example, if a central network DNS server is set a static IP address, and a remote location's local DNS server is defined, this host can be overridden at the remote location. At the remote location, the network is functional with a local DNS server, but uses the name set at the central network. A new host need not be created at the remote location. This simplifies creating and managing hosts and allows an administrator to better manage specific local requirements.</p> <ul style="list-style-type: none"> <li>• &lt;HOST-ALIAS-NAME&gt; - Specify the host alias name.</li> </ul> <p>Alias name should begin with '\$'.</p> |
| <b>&lt;HOST-IP&gt;</b>              | <p>Associates the network host's IP address with this host alias</p> <ul style="list-style-type: none"> <li>• &lt;HOST-IP&gt; - Specify the network host's IP address.</li> </ul> <p>Aliases defined at any given level can be overridden at the next lower levels. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

```
alias network <NETWORK-ALIAS-NAME> <NETWORK-ADDRESS/MASK>
```

|                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>network</b><br><b>&lt;NETWORK-ALIAS-NAME&gt;</b> | <p>Creates a new network alias for this profile. Or associates an existing network alias with this profile. A network alias configuration is utilized for an IP address on a particular network. Use this option to create unique Network aliases for different deployment scenarios. For example, if a central network ACL defines a network as 192.168.10.0/24, and a remote location's network range is 172.16.10.0/24, the ACL can be overridden at the remote location to suit their local (but remote) requirement.</p> <p>At the remote location, the ACL functions with the 172.16.10.0/24 network. A new ACL need not be created specifically for the remote deployment. This simplifies ACL definition and allows an administrator to better manage specific local requirements.</p> <ul style="list-style-type: none"> <li>• &lt;NETWORK-ALIAS-NAME&gt; - Specify the network alias name.</li> </ul> <p>Alias name should begin with '\$'.</p> |
| <b>&lt;NETWORK-ADDRESS/MASK&gt;</b>                 | <p>Associates a single network with this network alias</p> <ul style="list-style-type: none"> <li>• &lt;NETWORK-ADDRESS/MASK&gt; - Specify the network's address and mask.</li> </ul> <p>Aliases defined at any given level can be overridden at the next lower levels. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

```
alias network-group <NETWORK-GROUP-ALIAS-NAME> [address-range <STARTING-IP> to <ENDING-IP> {<STARTING-IP> to <ENDING-IP>} | host <HOST-IP> {<HOST-IP>} | network <NETWORK-ADDRESS/MASK> {<NETWORK-ADDRESS/MASK>}]
```

|                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>network</b><br><b>&lt;NETWORK-GROUP-ALIAS-NAME&gt;</b>                                                                                                     | <p>Creates a new network-group alias for this profile. Or associates an existing network-group alias with this profile.</p> <ul style="list-style-type: none"> <li>• &lt;NETWORK-GROUP-ALIAS-NAME&gt; - Specify the network-group alias name.</li> </ul> <p>Alias name should begin with '\$'.</p> <p>The network-group aliases are used in ACLs, to define the network-specific components. ACLs using aliases can be used across sites by re-defining the network-group alias elements at the device or profile level.</p> <p>After specifying the name, specify the following: a range of IP addresses, host addresses, or a range of network addresses.</p> <p>Aliases defined at any given level can be overridden at the next lower levels. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence.</p> |
| <b>address-range</b><br><b>&lt;STARTING-IP&gt;</b><br><b>to &lt;ENDING-IP&gt;</b><br><b>{&lt;STARTING-IP&gt;</b><br><b>to &lt;ENDING-IP&gt;</b><br><b>IP}</b> | <p>Associates a range of IP addresses with this network-group alias</p> <ul style="list-style-type: none"> <li>• &lt;STARTING-IP&gt; - Specify the first IP address in the range.</li> <li>• to &lt;ENDING-IP&gt; - Specify the last IP address in the range.</li> <li>• &lt;STARTING-IP&gt; to &lt;ENDING-IP&gt; - Optional. Specifies more than one range of IP addresses. A maximum of eight (8) IP address ranges can be configured.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

|                                                                              |                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>host</b> <HOST-IP><br>{<HOST-IP>}                                         | <p>Associates a single or multiple hosts with this network-group alias</p> <ul style="list-style-type: none"> <li>• &lt;HOST-IP&gt; – Specify the host's IP address.</li> <li>• &lt;HOST-IP&gt; – Optional. Specifies more than one host. A maximum of eight (8) hosts can be configured.</li> </ul>                                             |
| <b>network</b><br><NETWORK-<br>ADDRESS/MASK><br>{<NETWORK-<br>ADDRESS/MASK>} | <p>Associates a single or multiple networks with this network-group alias</p> <ul style="list-style-type: none"> <li>• &lt;NETWORK-ADDRESS/MASK&gt; – Specify the network's address and mask.</li> <li>• &lt;NETWORK-ADDRESS/MASK&gt; – Optional. Specifies more than one network. A maximum of eight (8) networks can be configured.</li> </ul> |

```
alias network-service <NETWORK-SERVICE-ALIAS-NAME> proto [<0-254>|<WORD>| eigrp|gre|igmp|
igp|ospf|vrrp] {(<1-65535>|<WORD>|bgp|dns|ftp|ftp-data|gopher| https|ldap|nntp|ntp|pop3|
proto|sip|smtp|sourceport [<1-65535>|<WORD>]|ssh| telnet|tftp|www)}
```

|                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>alias network-<br/>service</b><br><NETWORK-<br>SERVICE-ALIAS-<br>NAME>  | <p>Creates a new network-service alias for this profile. Or associates an existing network-service alias with this profile. A network service alias is a set of configurations that consist of protocol and port mappings. Both source and destination ports are configurable. For each protocol, up to 2 source port ranges and up to 2 destination port ranges can be configured. A maximum of 4 protocol entries can be configured per network service alias. &lt;NETWORK-SERVICE-ALIAS-NAME&gt; – Specify a network-service alias name.</p> <p><b>Note:</b> Alias name should begin with '\$'.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|                                                                            | <p>The network-service aliases are used in ACLs, to define the service-specific components. ACLs using aliases can be used across sites by re-defining the network-service alias elements at the device or profile level.</p> <p><b>Note:</b> Aliases defined at any given level can be overridden at the next lower levels. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>proto</b><br>[<0-254> <br><WORD> eigrp <br>gre  igmp igp <br>ospf vrrp] | <p>Use one of the following options to associate an Internet protocol with this network-service alias:</p> <ul style="list-style-type: none"> <li>• &lt;0-254&gt; – Identifies the protocol by its number. Specify the protocol number from 0 - 254. This is the number by which the protocol is identified in the Protocol field of the IPv4 header and the Next Header field of IPv6 header. For example, the User Datagram Protocol's (UDP) designated number is 17.</li> <li>• &lt;WORD&gt; – Identifies the protocol by its name. Specify the protocol name.</li> <li>• eigrp – Selects Enhanced Interior Gateway Routing Protocol (EIGRP). The protocol number 88.</li> <li>• gre – Selects Generic Routing Encapsulation (GRE). The protocol number is 47.</li> <li>• igmp – Selects Internet Group Management Protocol (IGMP). The protocol number is 2.</li> <li>• igp – Selects Interior Gateway Protocol (IGP). The protocol number is 9.</li> <li>• ospf – Selects Open Shortest Path First (OSPF). The protocol number is 89.</li> <li>• vrrp – Selects Virtual Router Redundancy Protocol (VRRP). The protocol number is 112.</li> </ul> |

|                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>{ (&lt;1-65535&gt;   &lt;WORD&gt;   bgp   dns   ftp   ftp- data   gopher   https   ldap   nntp   ntp   pop3   proto   sip   smtp   sourceport [&lt;1-65535&gt;   &lt;WORD&gt;]   ssh   telnet   tftp   www) }</pre> | <p>After specifying the protocol, you may configure a destination port for this service. These keywords are recursive and you can configure multiple protocols and associate multiple destination and source ports.</p> <ul style="list-style-type: none"> <li>• &lt;1-65535&gt; - Optional. Configures a destination port number from 1 - 65535</li> <li>• &lt;WORD&gt; - Optional. Identifies the destination port by the service name provided. For example, the secure shell (SSH) service uses TCP port 22.</li> <li>• bgp - Optional. Configures the default Border Gateway Protocol (BGP) services port (179)</li> <li>• dns - Optional. Configures the default Domain Name System (DNS) services port (53)</li> <li>• ftp - Optional. Configures the default File Transfer Protocol (FTP) control services port (21)</li> <li>• ldap - Optional. Configures the default Lightweight Directory Access Protocol (LDAP) services port (389)</li> <li>• ftp-data - Optional. Configures the default FTP data services port (20)</li> <li>• gopher - Optional. Configures the default gopher services port (70)</li> <li>• https - Optional. Configures the default HTTPS services port (443)</li> <li>• nntp - Optional. Configures the default Newsgroup (NNTP) services port (119)</li> <li>• ntp - Optional. Configures the default Network Time Protocol (NTP) services port (123)</li> <li>• proto - Optional. Use this option to select another Internet protocol in addition to the one selected in the previous step.</li> <li>• sip - Optional. Configures the default Session Initiation Protocol (SIP) services port (5060).</li> </ul> |
|                                                                                                                                                                                                                          | <ul style="list-style-type: none"> <li>• sourceport [&lt;1-65535&gt; &lt;WORD&gt;] - Optional. After specifying the destination port, you may specify a single or range of source ports. <ul style="list-style-type: none"> <li>• &lt;1-65535&gt; - Specify the source port from 1 - 65535.</li> <li>• &lt;WORD&gt; - Specify the source port range, for example 1-10.</li> </ul> </li> <li>• ssh - Optional. Configures the default SSH services port (22)</li> <li>• telnet - Optional. Configures the default Telnet services port (23)</li> <li>• tftp - Optional. Configures the default Trivial File Transfer Protocol (TFTP) services port (69)</li> <li>• www - Optional. Configures the default HTTP services port (80)</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

alias number <NUMBER-ALIAS-NAME> <0-4294967295>

|                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>alias number &lt;NUMBER-ALIAS- NAME&gt; &lt;0-4294967295&gt;</pre> | <p>Creates a number alias identified by the &lt;NUMBER-ALIAS-NAME&gt; keyword. Number aliases map a name to a numeric value. For example, 'alias number \$NUMBER 100'. In this example,</p> <ul style="list-style-type: none"> <li>• The number alias name is: \$NUMBER</li> <li>• The value assigned is: 100</li> </ul> <p>The value d by alias \$NUMBER, wherever used, is 100.</p> <ul style="list-style-type: none"> <li>• &lt;NUMBER-ALIAS-NAME&gt; - Specify the number alias name. <ul style="list-style-type: none"> <li>• &lt;0-4294967295&gt; - Specify the number, from 0 - 4294967295, assigned to the number alias created.</li> </ul> </li> </ul> <p><b>Note:</b> Alias name should begin with '\$'.</p> |
|-------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

alias string <STRING-ALIAS-NAME> <LINE>



|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>alias string</b><br><b>&lt;STRING-ALIAS-NAME&gt;</b> | <p>Creates a new string alias for this profile. Or associates an existing string alias with this profile. String aliases map a name to an arbitrary string value. Use this option to create unique string aliases for different deployment scenarios. For example, if the main domain at a remote location is called loc1.domain.com and at another deployment location it is called loc2.domain.com, the alias can be overridden at the remote location to suit the local (but remote) requirement. At one remote location, the alias functions with the loc1.domain.com domain and at the other with the loc2.domain.com domain.</p> <ul style="list-style-type: none"> <li>• &lt;STRING-ALIAS-NAME&gt; – Specify the string alias name. <ul style="list-style-type: none"> <li>• &lt;LINE&gt; – Specify the string value.</li> </ul> </li> </ul> <p><b>Note:</b> Alias name should begin with '\$'.</p> <p>Aliases defined at any given level can be overridden at the next lower levels. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence.</p> |
|---------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
alias vlan <VLAN-ALIAS-NAME> <1-4094>
```

|                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>alias vlan</b><br><b>&lt;VLAN-ALIAS-NAME&gt;</b> | <p>Creates a new VLAN alias for this profile. Or associates an existing VLAN alias with this profile. A VLAN alias maps a name to a VLAN ID. A VLAN alias is a configuration for optimal VLAN re-use and management for local and remote deployments. Use this option to create unique VLANs aliases for different deployment scenarios. For example, if a VLAN ID is set as 10 for the central network, and the VLAN is set as 26 at a remote location, the VLAN can be overridden at the remote location using an alias.</p> |
|                                                     | <p>At the remote location, the network is functional with an ID of 26, but utilizes the name defined at the central local network. A new VLAN need not be created specifically at the remote location.</p> <ul style="list-style-type: none"> <li>• &lt;VLAN-ALIAS-NAME&gt; – Specify the VLAN alias name.</li> </ul> <p><b>Note:</b> Alias name should begin with '\$'.</p>                                                                                                                                                   |
| <b>&lt;1-4094&gt;</b>                               | <p>Maps the VLAN alias to a VLAN ID</p> <ul style="list-style-type: none"> <li>• &lt;1-4094&gt; – Specify the VLAN ID from 1 - 4094.</li> </ul> <p>Aliases defined at any given level can be overridden at the next lower levels. For example, a global alias can be redefined on a selected set of RF Domains, profiles, or devices. Overrides applied at the device level take precedence.</p>                                                                                                                               |

## Example

The following example shows the global aliases configured. Note the network-service alias '\$kerberos' settings.

```
nx9500-6C8809(config)#show running-config | include alias
alias network-group $NetGrpAlias address-range 192.168.13.7 to 192.168.13.16 192.168.13.20
to 192.168.13.25
alias network-group $NetGrpAlias network 192.168.13.0/24 192.168.16.0/24
alias network $NetworkAlias 192.168.13.0/24
alias host $HostAlias 192.168.13.10
alias address-range $AddRanAlias 192.168.13.10 to 192.168.13.13
alias network-service $kerberos network tcp 23 proto udp 25
alias vlan $VlanAlias 1
alias string $AREA Ecospace
alias string $IN-Blr-EcoSpace-Floor-4 IBEF4
alias encrypted-string $READ 2 CdO6glQ9w29hybKxfbd6JwAAAAa7lKMBMk9EiDQfFRf9kegO
alias hashed-string $PriMode 1
faffdde27cb49ad634ea20df4f7c8ef2685894d10ffcb1b2efba054112ecfc75
nx9500-6C8809(config)#
```

The following examples show the overrides applied to the network-service alias '\$kerberos' at the profile level:

```
nx9500-6C8809(config-profile-testRFS4k)#alias network-service $kerberos proto tcp 22 proto udp 389
```

The following example shows the overrides applied to the network-service alias '\$kerberos' at the profile level:

```
nx9500-6C8809(config-profile-testRFS4k)#show running-config | include alias
alias network-group $NetGrpAlias address-range 192.168.13.7 to 192.168.13.16 192.168.13.20
to 192.168.13.25
alias network-group $NetGrpAlias network 192.168.13.0/24 192.168.16.0/24
alias network $NetworkAlias 192.168.13.0/24
alias host $HostAlias 192.168.13.10
alias address-range $AddRanAlias 192.168.13.10 to 192.168.13.13
alias network-service $kerberos proto tcp 22 proto udp 389
alias vlan $VlanAlias 1
alias string $AREA Ecospace
alias string $IN-Blr-EcoSpace-Floor-4 IBEF4
alias encrypted-string $READ 2 /Mfbt1Et8XRhybKxfbd6JwAAAAZ9yrIYq7mNl4+gNNiimIZI
alias hashed-string $PriMode 1
fa9f9d27cb49ad634ea20df4f7c8ef2685894d10ffcb1b2efba054112ecfc75
alias network-service $kerberos proto tcp 88 proto udp 389
nx9500-6C8809(config-profile-testRFS4k)#
```

## Related Commands

|                              |                                         |
|------------------------------|-----------------------------------------|
| <code>no</code> on page 1200 | Removes a specified alias configuration |
|------------------------------|-----------------------------------------|

### *application-policy*

[Profile Config Commands](#) on page 862

Associates an application policy with this profile. This command is also applicable to the device configuration mode. When associated, the application policy allows wireless clients (MUs) to always find the RADIUS-supplied application policy in the dataplane.

An application policy defines the actions executed on recognized HTTP (Facebook), enterprise (Webex) and peer-to-peer (gaming) applications or application-categories. The following are the actions that can be applied in an application policy:

- Allow - Allows packets for a specific application and its defined category type (for e.g., social networking)
- Deny - Denies (restricts) packets to a specific application and its defined category type
- Mark - Marks recognized packets with DSCP/8021p value
- Rate-limit - Rate limits packets from specific application type

For more information on configuring an application policy, see [application-policy](#) on page 267.

### Supported in the following platforms:

- Access Points — AP7522, AP7532
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

## Syntax

```
application-policy radius <APP-POLICY-NAME>
```

## Parameters

```
application-policy radius <APP-POLICY-NAME>
```

|                                                          |                                                                                                                                                                                                                               |
|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>application-policy radius &lt;APP-POLICY-NAME&gt;</b> | Associates a RADIUS server provided application policy with this profile <ul style="list-style-type: none"><li>• &lt;APP-POLICY-NAME&gt; - Specify the application policy name (should be existing and configured).</li></ul> |
|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Example

```
nx9500-6C8809(config-profile-testNX9500)#application-policy radius Bing
```

```
nx9500-6C8809(config-profile-testNX9500)#show context include-factory | include application-policy
 application-policy radius Bing
nx9500-6C8809(config-profile-testNX9500)#
```

```
nx9500-6C8809(config-application-Bing)#Show context application Bing
 app-category streaming
 use url-list Bing
nx9500-6C8809(config-application-Bing)#
```

## Related Commands

|                                 |                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------|
| <a href="#">no</a> on page 1200 | Removes the RADIUS-server provided application policy associated with this profile |
|---------------------------------|------------------------------------------------------------------------------------|

*area*

[Profile Config Commands](#) on page 862

Sets the system's area of location (the physical area of deployment)

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

## Syntax

```
area <WORD>
```

## Parameters

```
area <WORD>
```

|                          |                                                                                                                                                              |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>area &lt;WORD&gt;</b> | Sets the system's area of location <ul style="list-style-type: none"><li>• &lt;WORD&gt; - Specify the area name (should not exceed 64 characters).</li></ul> |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Example

```
nx9500-6C8809(config-profile-default-rfs4000)#area Ecospace

nx9500-6C8809(config-profile-default-rfs4000)#show context
profile rfs4000 default-rfs4000
 bridge vlan 1
 ip igmp snooping
 ip igmp snooping querier
 area Ecospace
 autoinstall configuration
 autoinstall firmware
 crypto ikev1 policy ikev1-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 interface mel
 interface gel
--More--
nx9500-6C8809(config-profile-default-rfs4000)#
```

## Related Commands

|                              |                                 |
|------------------------------|---------------------------------|
| <code>no</code> on page 1200 | Resets the configured area name |
|------------------------------|---------------------------------|

## *arp*

[Profile Config Commands](#) on page 862

Adds a static Address Resolution Protocol (ARP) IP address in the ARP cache

The ARP protocol maps an IP address to a hardware MAC address recognized on the network. ARP provides protocol rules for making this correlation and providing address conversion in both directions.

When an incoming packet destined for a host arrives, ARP finds a physical host or MAC address that matches the IP address. ARP looks in its ARP cache and, if it finds the address, provides it so the packet can be converted to the right packet length, formatted, and sent to its destination. If no entry is found for the IP address, ARP broadcasts a request packet in a special format on the LAN to locate a device that recognizes the IP address. A device that recognizes the IP address as its own returns a reply indicating it. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
arp [<IP>|timeout]
```

```
arp <IP> <MAC> arpa [<L3-INTERFACE-NAME>|pppoe1|vlan <1-4094>|wwan1|
serial <1-4> <1-1> <1-1>] {dhcp-server/router}
```

```
arp timeout <15-86400>
```

### Parameters

```
arp <IP> <MAC> arpa [<L3-INTERFACE-NAME>|pppoe1|vlan <1-4094>|wwan1|serial <1-4> <1-1>
<1-1>] {dhcp-server/router}
```

|                                  |                                                                                                                                                                                                                                                |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>arp &lt;IP&gt;</b>            | Adds a static ARP IPv4 address in the ARP cache <ul style="list-style-type: none"> <li>&lt;IP&gt; - Specify the static IP address.</li> </ul>                                                                                                  |
| <b>&lt;MAC&gt;</b>               | Specify the MAC address associated with the IP and the Switch Virtual Interface (SVI).                                                                                                                                                         |
| <b>arpa</b>                      | Sets ARP encapsulation type to ARPA                                                                                                                                                                                                            |
| <b>&lt;L3-INTERFACE-NAME&gt;</b> | Configures static ARP entry for a specified router interface <ul style="list-style-type: none"> <li>&lt;L3-INTERFACE-NAME&gt; - Specify the router interface name.</li> </ul>                                                                  |
| <b>pppoe1</b>                    | Configures static ARP entry for PPP over Ethernet interface                                                                                                                                                                                    |
| <b>vlan &lt;1-4094&gt;</b>       | Configures static ARP entry for a VLAN interface <ul style="list-style-type: none"> <li>&lt;1-4094&gt; - Specify a SVI VLAN ID from 1 - 4094.</li> </ul>                                                                                       |
| <b>wwan1</b>                     | Configures static ARP entry for Wireless WAN interface                                                                                                                                                                                         |
| <b>{dhcp-server   router}</b>    | The following keywords are common to all off the above interface types: <ul style="list-style-type: none"> <li>dhcp-server - Optional. Sets ARP entries for a DHCP server</li> <li>router - Optional. Sets ARP entries for a router</li> </ul> |

```
arp timeout <15-86400>
```

|                                     |                                                                                                                                                                                                      |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>arp timeout &lt;15-86400&gt;</b> | Sets ARP entry timeout <ul style="list-style-type: none"> <li>&lt;TIME&gt; - Sets the ARP entry timeout in seconds. Specify a value from 15 - 86400 seconds. The default is 3600 seconds.</li> </ul> |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Example

```
nx9500-6C8809(config-profile-default-rfs4000)#arp timeout 2000
```

```
nx9500-6C8809(config-profile-default-rfs4000)#show context
profile rfs4000 default-rfs4000
 bridge vlan 1
 bridging-mode isolated-tunnel
 ip igmp snooping
 ip igmp snooping querier
 arp timeout 2000
 crypto ikev1 policy ikev1-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 interface me1
 interface ge1
```

```

ip dhcp trust
qos trust dscp
qos trust 802.1p
interface ge2
ip dhcp trust
--More--
nx9500-6C8809(config-profile-default-rfs4000)#

```

## Related Commands

|                              |                                     |
|------------------------------|-------------------------------------|
| <code>no</code> on page 1200 | Removes an entry from the ARP cache |
|------------------------------|-------------------------------------|

## auto-learn

[Profile Config Commands](#) on page 862

Enables controllers or service platforms to maintain a local configuration record of devices requesting adoption and provisioning. The command also enables learning of a device's host name via DHCP options.

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
auto-learn [host-name-via-dhcp <WORD>|staging-config]
```

### Parameters

```
auto-learn [host-name-via-dhcp <WORD>|staging-config]
```

|                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>auto-learn</b><br><b>[host-name-</b><br><b>via-dhcp</b><br><b>&lt;WORD&gt;  </b><br><b>staging-</b><br><b>config]</b> | <p>Enables auto-learning of:</p> <ul style="list-style-type: none"> <li>• host-name-via-dhcp - A device's host name via DHCP option. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Provide the optional template with substitution token. For example, 'outdoor-\$DHCP[1:3]-ap', where the \$DHCP token references DHCP Option value received by the adopting device. The \$DHCP token should be present. This option is disabled by default.</li> </ul> </li> <li>• staging-config - The network configuration of devices requesting adoption. This option is enabled by default. For dependent access points that are pre-staged prior to deployment, it is recommended that the auto-learn-staging-config parameter remains enabled so that hostnames, VLAN and IP addressing configuration can be maintained upon initial adoption. However, if dependent access points are to be centrally managed and configured, it is recommended that the auto-learn-staging-config parameter be disabled</li> </ul> |
|--------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Example

```
nx9500-6C8809(config-profile-test)#auto-learn staging-config
```

```
nx9500-6C8809(config-profile-test)#show context include-factory | include auto-learn
auto-learn staging-config
```

```
no auto-learn host-name-via-dhcp
nx9500-6C8809(config-profile-test)#
```

## Related Commands

|                                 |                                                                                  |
|---------------------------------|----------------------------------------------------------------------------------|
| <a href="#">no</a> on page 1200 | Disables automatic recognition of devices' hostname and devices pending adoption |
|---------------------------------|----------------------------------------------------------------------------------|

### *autogen-uniqueid*

[Profile Config Commands](#) on page 862

Auto-generates a unique ID for devices using this profile. When executed in the device configuration mode, this command generates a unique ID for the logged device. A device's unique ID is a combination of a user-defined string (prefix, suffix, or both) and a substitution token. The WiNG implementation provides two built-in substitution tokens: \$SN and \$MiNT-ID that represent the device's serial number and MiNT-ID respectively. The value referenced by these substitution tokens are internally retrieved and combined with the user-defined string to auto generate a unique identity for the device.

The general format of this command is: <PREFIX><SUBSTITUTION-TOKEN><SUFFIX>. You can provide both (prefix and suffix) or just a prefix or suffix.

For example, given the following set of inputs:

- user-defined prefix – TestAP6522
- substitution token – \$SN

The unique ID is generated using TestAP6522\$SN, where \$SN is replaced with the device's serial number.

When executed on an AP6522 (having serial number B4C7996C8809), the autogen-uniqueid TestAP6522\$SN command generates the unique ID: TestAP6522B4C7996C8809. When configured on an AP6522 profile, all AP6522s using the profile auto-generate a unique ID in which the device's serial number is preceded by the string 'TestAP6522'.

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
autogen-uniqueid <WORD>
```

### Parameters

```
autogen-uniqueid <WORD>
```

**autogen-uniqueid**  
**<WORD>**

Auto-generates a device's unique ID (not exceeding 64 characters in length)  
The ID generated is a combination of the text provided and the value referenced through the substitution token \$SN or \$MiNT-ID. Where ever the autogen-uniqueid is used the device's serial number OR MiNT-ID is referenced depending on the substitution token used.

- <WORD> - Specify a auto generate unique ID format using one of the following substitution tokens:

Available tokens:

- \$SN - references SERIAL NUMBER of the device
- \$MINT-ID - references MINT-ID of the device

For example, Test-\$SN-TechPubs. In this example 'Test' and 'TechPubs' represent the user-defined prefix and suffix respectively. And \$SN is the substitution token.

### Example

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#autogen-uniqueid Test-$MiNT-ID-TechPubs
```

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context
```

```
nx9000 B4-C7-99-6C-88-09
```

```
 use profile default-nx9000
```

```
 use rf-domain TechPubs
```

```
 hostname nx9500-6C8809
```

```
 license AAP
```

```
66069c24b3bb1259b34ff016c723a9e299dd408f0ff891e7c5f7e279a382648397d6b3e975e356a1
```

```
 license HTANLT
```

```
66069c24b3bb1259eb36826cab3cc83999dd408f0ff891e74b62b2d3594f0b3dde7967f30e49e497
```

```
 timezone Asia/Calcutta
```

```
 use database-policy default
```

```
 use nsight-policy noc
```

```
 autogen-uniqueid Test-$MiNT-ID-TechPubs
```

```
 ip default-gateway 192.168.13.2
```

```
 device-upgrade auto rfs4000 ap81xx ap71xx ap7562 ap7532
```

```
 interface ge1
```

```
 switchport mode access
```

```
 switchport access vlan 1
```

```
 interface ge2
```

```
 --More--
```

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```

### Related Commands

**no** on page 1200

When executed in the device configuration mode, removes the device's autogen-uniqueid. When executed in the profile configuration mode, removes the autogen-uniqueid on all devices using the profile.

*autoinstall*

[Profile Config Commands](#) on page 862

Automatically installs firmware image and startup configuration parameters on to the selected device.

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000



- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
autoinstall [configuration|firmware|start-interval <WORD>]
```

### Parameters

```
autoinstall [configuration|firmware|start-interval <WORD>]
```

|                                    |                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>configuration</b>               | Autoinstalls startup configuration. Setup parameters are automatically configured on devices using this profile. This option is disabled by default.                                                                                                                                                                                                                                           |
| <b>firmware</b>                    | Autoinstalls firmware image. Firmware images are automatically installed on devices using this profile. This option is disabled by default.                                                                                                                                                                                                                                                    |
| <b>start-interval &lt;WORD&gt;</b> | Configures the interval between system boot and start of autoinstall process (this is the time, from system boot, after which autoinstall should start) <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specify the interval in minutes. The default is 10 minutes.</li> </ul> <p><b>Note:</b> Zero (0) implies firmware or startup configuration installation can start any time.</p> |

### Example

```
nx9500-6C8809(config-profile-default-rfs4000)#autoinstall configuration
```

```
nx9500-6C8809(config-profile-default-rfs4000)#autoinstall firmware
```

```
nx9500-6C8809(config-profile-default-rfs4000)#show context
profile rfs4000 default-rfs4000
bridge vlan 1
 bridging-mode isolated-tunnel
 ip igmp snooping
 ip igmp snooping querier
arp timeout 2000
autoinstall configuration
autoinstall firmware
crypto ikev1 policy ikev1-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ikev2 policy ikev2-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
crypto ikev1 remote-vpn
crypto ikev2 remote-vpn
```

```
--More--
```

```
nx9500-6C8809(config-profile-default-rfs4000)#
```

### Related Commands

|                        |                                    |
|------------------------|------------------------------------|
| <b>no</b> on page 1200 | Disables the auto install settings |
|------------------------|------------------------------------|

*bridge*

[Profile Config Commands](#) on page 862

The following table summarizes Ethernet bridge configuration commands:

| Command                                               | Description                                        |
|-------------------------------------------------------|----------------------------------------------------|
| <a href="#">bridge</a> on page 886                    | Enables Ethernet bridge configuration context      |
| <a href="#">bridge-vlan-mode commands</a> on page 888 | Summarizes bridge VLAN configuration mode commands |

## bridge

[bridge](#) on page 885

Configures VLAN Ethernet bridging parameters. Use this command to configure a Bridge NAT or Bridge VLAN settings

Configuring bridge Network Address Translation (NAT) parameters, allows management of Internet traffic originating at a remote site. In addition to traditional NAT functionality, bridge NAT provides a means of configuring NAT for bridged traffic through an access point. NAT rules are applied to bridged traffic through the access point, and matching packets are NATed to the WAN link instead of being bridged on their way to the router. Using bridge NAT, a tunneled VLAN (extended VLAN) is created between the NOC and a remote location. When a remote client needs to access the Internet, Internet traffic is routed to the NOC, and from there routed to the Internet. This increases the access time for the end user on the client. To resolve latency issues, bridge NAT identifies and segregates traffic heading towards the NOC and outwards towards the Internet. Traffic towards the NOC is allowed over the secure tunnel. Traffic towards the Internet is switched to a local WLAN link with access to the Internet.

A Virtual LAN (VLAN) is a separately administrated virtual network within the same physical managed network. VLANs are broadcast domains defined within wireless controllers or service platforms to allow control of broadcast, multicast, unicast, and unknown unicast within a layer 2 device. Administrators often need to route traffic between different VLANs. Bridging VLANs are only for non-routable traffic, like tagged VLAN frames destined to some other device, which will untag it. When a data frame is received on a port, the VLAN bridge determines the associated VLAN based on the port of reception. Using forwarding database information, the bridge VLAN forwards the data frame on the appropriate port(s). VLANs are useful to set separate networks to isolate some computers from others, without actually having to have separate cabling and Ethernet switches. Controllers can do this on their own, without need for the computer or other gear to know itself what VLAN it is on (this is called port-based VLAN, since it is assigned by port of the switch). Another common use is to put specialized devices like VoIP Phones on a separate network for easier configuration, administration, security, or service quality.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
bridge [nat|vlan]
```

```
bridge nat source list <IP-ACCESS-LIST-NAME> precedence <1-500> interface
[<LAYER3-INTERFACE-NAME>|pppoe1|vlan <1-4094>|wan1] [(address|interface|
overload|pool <NAT-POOL-NAME>)]
```

```
bridge vlan [<1-4094>|<VLAN-ALIAS-NAME>]
```

#### Parameters

```
bridge nat source list <IP-ACCESS-LIST-NAME> precedence <1-500> interface [<LAYER3-INTERFACE-NAME>|pppoe1|vlan <1-4094>|wwan1] [(address|interface|overload|pool <NAT-POOL-NAME>)]
```

|                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>nat</b>                                                                         | Configures bridge NAT parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>source</b>                                                                      | Configures NAT source addresses                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>list &lt;IP-ACCESS-LIST-NAME&gt;</b><br><b>precedence &lt;1-500&gt;</b>         | Associates an access control list (ACL) with this bridge NAT policy. The ACL specifies the IP address permit/deny rules applicable to this bridge NAT policy. <ul style="list-style-type: none"> <li>&lt;IP-ACCESS-LIST-NAME&gt; - Specify access list name.</li> <li>precedence &lt;1-500&gt; - Specifies a precedence value for this bridge NAT policy.</li> </ul>                                                                                                                                                                                                                                       |
| <b>interface [&lt;LAYER3-INTERFACE-NAME&gt; pppoe1 vlan &lt;1-4094&gt;  wwan1]</b> | Selects one of the following as the primary interface (between the source and destination points): <ul style="list-style-type: none"> <li>&lt;LAYER3-INTERFACE-NAME&gt; - A router interface. Specify interface name.</li> <li>pppoe1 - A PPP over Ethernet interface.</li> <li>vlan &lt;1-4094&gt; - A VLAN interface. Specify the VLAN interface index from 1 - 4094.</li> <li>wwan1 - A Wireless WAN interface.</li> </ul>                                                                                                                                                                              |
| <b>[( address   interface   overload   pool &lt;NAT-POOL-NAME&gt; )]</b>           | The following keywords are recursive and common to all interface types: <ul style="list-style-type: none"> <li>address - Configures the interface IP address used for NAT</li> <li>interface - Configures the failover interface (default setting)</li> <li>overload - Enables use of one global address for multiple local addresses (terminates command)</li> <li>pool &lt;NAT-POOLNAME&gt; - Configures the NAT pool used with this bridge NAT policy. Specify the NAT pool name. For more information on configuring a NAT pool, see <a href="#">nat-pool-config-instance</a> on page 1160.</li> </ul> |

```
bridge vlan [<1-4094>|<VLAN-ALIAS-NAME>]
```

|                                     |                                                                                                                                                                                                  |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vlan &lt;1-4094&gt;</b>          | Configures the numerical identifier for the Bridge VLAN when it was initially created. <ul style="list-style-type: none"> <li>&lt;1-4094&gt; - Specify a VLAN index from 1 - 4094.</li> </ul>    |
| <b>vlan &lt;VLAN-ALIAS-NAME&gt;</b> | Configures the VLAN alias (should be existing and configured) identifying the bridge VLAN <ul style="list-style-type: none"> <li>&lt;VLAN-ALIAS-NAME&gt; - Specify a VLAN alias name.</li> </ul> |

#### Usage Guidelines

Creating customized filter schemes for bridged networks limits the amount of unnecessary traffic processed and distributed by the bridging equipment.

If a bridge does not hear Bridge Protocol Data Units (BPDUs) from the root bridge within the specified interval, defined in the max-age (seconds) parameter, assume the network has changed and recomputed the spanning-tree topology.

#### Example

```
nx9500-6C8809(config-profile-default-rfs4000)#bridge vlan 1
nx9500-6C8809(config-profile-default-rfs4000-bridge-vlan-1)#?
Bridge VLAN Mode commands:
```

| Bridge VLAN Mode commands:                |                                                                                     |
|-------------------------------------------|-------------------------------------------------------------------------------------|
| bridging-mode                             | Configure how packets on this VLAN are bridged                                      |
| captive-portal                            | Captive Portal                                                                      |
| captive-portal-enforcement                | Enable captive-portal enforcement on this extended VLAN                             |
| description                               | Vlan description                                                                    |
| edge-vlan                                 | Enable edge-VLAN mode                                                               |
| firewall                                  | Enable vlan firewall(IPv4)                                                          |
| http-analyze                              | Forward URL and Data to controller                                                  |
| ip                                        | Internet Protocol (IP)                                                              |
| ipv6                                      | Internet Protocol version 6 (IPv6)                                                  |
| l2-tunnel-broadcast-optimization          | Enable broadcast optimization                                                       |
| l2-tunnel-forward-additional-packet-types | Forward additional packet types not normally forwarded by l2 broadcast optimization |
| mac-auth                                  | Enable mac-auth for this bridge vlan                                                |
| name                                      | Vlan name                                                                           |
| no                                        | Negate a command or set its defaults                                                |
| stateful-packet-inspection-l2             | Enable stateful packet inspection in layer2 firewall                                |
| registration                              | Enable dynamic registration of device (or) user                                     |
| tunnel                                    | Vlan tunneling settings                                                             |
| tunnel-over-level2                        | Tunnel extended VLAN traffic over level 2 MiNT links                                |
| use                                       | Set setting to use                                                                  |
| clrscr                                    | Clears the display screen                                                           |
| commit                                    | Commit all changes made in this session                                             |
| do                                        | Run commands from Exec mode                                                         |
| end                                       | End current mode and change to EXEC mode                                            |
| exit                                      | End current mode and down to previous mode                                          |
| help                                      | Description of the interactive help system                                          |
| revert                                    | Revert changes                                                                      |
| service                                   | Service Commands                                                                    |
| show                                      | Show running system information                                                     |
| write                                     | Write running configuration to memory or terminal                                   |

nx9500-6C8809(config-profile-default-rfs4000-bridge-vlan-1)#

## bridge-vlan-mode commands

[bridge](#) on page 885

The following table summarizes bridge VLAN configuration mode commands:

**Table 34: Bridge VLAN Config Mode Commands**

| Command                                                               | Description                                                                                                                                                                                |
|-----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">bridging-mode</a> on page 889                             | Configures how packets on this VLAN are bridged                                                                                                                                            |
| <a href="#">captive-portal</a> on page 890                            | Enables IP packet snooping on wired captive portals, and also configures the subnet to snoop                                                                                               |
| <a href="#">captive-portal-enforcement</a> on page 891                | Enables auto-enforcement of captive portal rules on this extended VLAN interface                                                                                                           |
| <a href="#">description</a> on page 892                               | Configures VLAN bridge description                                                                                                                                                         |
| <a href="#">edge-vlan</a> on page 893                                 | Enables edge VLAN mode                                                                                                                                                                     |
| <a href="#">firewall</a> on page 893                                  | Enables firewall on this bridge VLAN interface                                                                                                                                             |
| <a href="#">http-analyze</a> on page 894                              | Enables the analysis of URLs and data traffic on this Bridge VLAN                                                                                                                          |
| <a href="#">ip</a> on page 895                                        | Configures IP components                                                                                                                                                                   |
| <a href="#">ipv6</a> on page 898                                      | Configures IPv6 components                                                                                                                                                                 |
| <a href="#">l2-tunnel-broadcast-optimization</a> on page 901          | Enables broadcast optimization                                                                                                                                                             |
| <a href="#">l2-tunnel-forward-additional-packet-types</a> on page 902 | Enables forwarding of WNMP (Wireless Network Management Protocol) packets across L2 tunnels. These WNMP packets are normally not forwarded if L2 tunnel broadcast optimization is enabled. |
| <a href="#">mac-auth</a> on page 902                                  | Enables MAC authentication for Extended VLAN and Tunneled traffic (both MiNT and L2TPv3)                                                                                                   |
| <a href="#">name</a> on page 904                                      | Configures a name for the selected Bridge VLAN                                                                                                                                             |
| <a href="#">no</a> on page 909                                        | Negates a command or reverts settings to their default                                                                                                                                     |
| <a href="#">stateful-packet-inspection-l2</a> on page 906             | Enables stateful packet inspection in the layer 2 fire wall                                                                                                                                |
| <a href="#">registration</a> on page 904                              | Enables forwarding of bridge-vlan information (such as, name and vlan) to the ExtremeGuest (EGuest) server.                                                                                |
| <a href="#">tunnel</a> on page 907                                    | Enables tunneling of unicast messages to unknown MAC destinations, on the selected VLAN bridge                                                                                             |
| <a href="#">tunnel-over-level2</a> on page 908                        | Enables extended VLAN traffic over level 2 MiNT links                                                                                                                                      |
| <a href="#">use</a> on page 911                                       | Associates a captive-portal, access control list (IP, IPv6, or MAC), and a URL filter with this bridge VLAN                                                                                |

bridging-mode

[bridge-vlan-mode commands](#) on page 888

Configures how packets are bridged on the selected VLAN

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
bridging-mode [auto|isolated-tunnel|local|tunnel]
```

#### Parameters

```
bridging-mode [auto|isolated-tunnel|local|tunnel]
```

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>bridging-mode</b>   | Configures the VLAN bridging mode                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>auto</b>            | Automatically selects the bridging mode to match the WLAN, VLAN and bridging mode configurations. When selected, the controller or access point determines the best bridging mode for the VLAN. (default setting)                                                                                                                                                                                                                                                                                                                                                      |
| <b>isolated-tunnel</b> | Bridges packets between local Ethernet ports and local radios, and passes tunneled packets through without de-tunneling<br>Select this option for a dedicated tunnel for bridging VLAN traffic.                                                                                                                                                                                                                                                                                                                                                                        |
| <b>local</b>           | Bridges packets normally between local Ethernet ports and local radios (if any)<br>Local mode is typically configured in remote branch offices where traffic on remote private LAN segments need to be bridged locally. Local mode implies that traffic, wired and wireless, is to be bridged locally.                                                                                                                                                                                                                                                                 |
| <b>tunnel</b>          | Bridges packets between local Ethernet ports, local radios, and tunnels to other APs, wireless controllers, or service platforms<br>Select this option to use a shared tunnel for bridging VLAN traffic.<br>In tunnel mode, the traffic at the AP is always forwarded through the best path. The APs decide the best path to reach the destination and forward packets accordingly. Setting the VLAN to tunnel mode ensures packets are bridged between local Ethernet ports, any local radios, and tunnels to other APs, wireless controllers, and service platforms. |

#### Usage Guidelines

ACLs can only be used with tunnel or isolated-tunnel modes. They do not work with the local and automatic modes.

#### Example

```
nx9500-6C8809(config-profile-default-rfs4000-bridge-vlan-1)#bridging-mode isolated-tunnel

nx9500-6C8809(config-profile-default-rfs4000-bridge-vlan-1)#show context
 bridge vlan 1
 bridging-mode isolated-tunnel
 ip igmp snooping
 ip igmp snooping querier
nx9500-6C8809(config-profile-default-rfs4000-bridge-vlan-1)#
```

#### Related Commands

|                                |                              |
|--------------------------------|------------------------------|
| <a href="#">no</a> on page 909 | Resets bridging mode to auto |
|--------------------------------|------------------------------|

[captive-portal](#)

[bridge-vlan-mode commands](#) on page 888

Enables IP (IPv4 and IPv6) packet snooping on wired captive portals, and also configures the subnet to snoop. When enabled, IP packets received from wired captive portal clients, on the specified subnet, are snooped to learn IP to MAC mapping.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
captive-portal [ipv4-snooping|ipv6-snooping] subnet <IPv4/M|IPv6/M>
{excluded-address <IPv4|IPv6>}
```

Parameters

```
captive-portal [ipv4-snooping|ipv6-snooping] subnet <IPv4/M|IPv6/M> {excluded-address
<IPv4|IPv6>}
```

|                                                                          |                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>captive-portal</b><br><b>[ipv4-snooping]</b><br><b>ipv6-snooping]</b> | Enables snooping of IPv4 or IPv6 packets (based on the option selected) for wired captive portal clients                                                                                                                                                                                                                                   |
| <b>subnet &lt;IPv4/M IPv6/M&gt;</b>                                      | Enables IPv4 or IPv6 packet snooping on a specified subnet <ul style="list-style-type: none"> <li>• &lt;IPv4/M IPv6/M&gt; – Specify the subnet address in the A.B.C.D/M or X::X:X/M format to identify an IPv4 or IPv6 subnet respectively. When specified, this is the IPv4/IPv6 subnet on which IP packets are to be snooped.</li> </ul> |
| <b>excluded-address &lt;IPv4 IPv6&gt;</b>                                | Optional. Configures the IPv4 or IPv6 address excluded from snooping within the specified IPv4 IPv6 subnet. <ul style="list-style-type: none"> <li>• &lt;IPv4 IPv6&gt; – Specify the IPv4 or IPv6 address. Use this parameter to configure the gateway's address.</li> </ul>                                                               |

Example

```
nx9500-6C8809(config-profile NX9500Test-bridge-vlan-4)#captive-portal ip-snooping subnet
192.168.13.0/24 excluded-address 192.168.13.7
```

```
nx9500-6C8809(config-profile NX9500Test-bridge-vlan-4)#show context
bridge vlan 4
captive-portal ip-snooping subnet 192.168.13.0/24 excluded-address 192.168.13.7
ip igmp snooping
ip igmp snooping querier
ipv6 mld snooping
ipv6 mld snooping querier
nx9500-6C8809(config-profile NX9500Test-bridge-vlan-4)#
```

Related Commands

|                       |                                                      |
|-----------------------|------------------------------------------------------|
| <b>no</b> on page 909 | Disables IP packet snooping on wired captive portals |
|-----------------------|------------------------------------------------------|

captive-portal-enforcement

[bridge-vlan-mode commands](#) on page 888

Enables auto-enforcement of captive portal rules on this extended VLAN interface. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
captive-portal-enforcement {fall-back}
```

Parameters

```
captive-portal-enforcement {fallback}
```

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>captive-portal-enforcement</b> | Enables auto-enforcement of captive portal access permission rules to data transmitted over this extended VLAN interface. When enforced, wired network users can pass traffic through the captive portal without being redirected to an authentication page. Authentication instead takes place when the RADIUS server is queried against the wired user's MAC address. If the MAC address is in the RADIUS server's user database, the user is allowed access.<br>A captive portal is an access policy for providing temporary and restrictive access using a standard Web browser. Captive portals capture and re-direct a wired/wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access the network. |
| <b>fall-back</b>                  | Optional. If enabling source MAC authentication for Extended VLAN and tunneled traffic on this bridge VLAN, use this option to enforce captive-portal authentication as the fall-back mode of authentication in case MAC authentication fails.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

Example

```
nx9500-6C8809(config-profile testAP7602-bridge-vlan-20)#show context
bridge vlan 20
captive-portal-enforcement
ip igmp snooping
ip igmp snooping querier
ipv6 mld snooping
ipv6 mld snooping querier
nx9500-6C8809(config-profile testAP7602-bridge-vlan-20)#
```

Related Commands

|                       |                                                                                   |
|-----------------------|-----------------------------------------------------------------------------------|
| <b>no</b> on page 909 | Disables auto-enforcement of captive portal rules on this extended VLAN interface |
|-----------------------|-----------------------------------------------------------------------------------|

description

[bridge-vlan-mode commands](#) on page 888

Configures this extended VLAN's description

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7632, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax



`description <WORD>`

Parameters

`description <WORD>`

|                                           |                                                                                                                                                                                                                                                                                               |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>description</b><br><b>&lt;WORD&gt;</b> | Configures a description for this VLAN bridge <ul style="list-style-type: none"><li>• <code>&lt;WORD&gt;</code> – Enter a description. The description should be unique to the VLAN's specific configuration to help differentiate it from other VLANs with similar configurations.</li></ul> |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Example

```
nx9500-6C8809(config-profile-default-rfs4000-bridge-vlan-1)#description "This is a description for the bridged VLAN"
```

```
nx9500-6C8809(config-profile-default-rfs4000-bridge-vlan-1)#show context
 bridge vlan 1
 description "This is a description for the bridged VLAN"
 bridging-mode isolated-tunnel
 ip igmp snooping
 ip igmp snooping querier
nx9500-6C8809(config-profile-default-rfs4000-bridge-vlan-1)#
```

Related Commands

|                             |                            |
|-----------------------------|----------------------------|
| <code>no</code> on page 909 | Removes VLAN's description |
|-----------------------------|----------------------------|

edge-vlan

[bridge-vlan-mode commands](#) on page 888

Enables the edge VLAN mode. In the edge VLAN mode, a protected port does not forward traffic to another protected port on the same wireless controller or service platform. This feature is enabled by default.

Supported in the following platforms:

- Access Points – AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers – RFS4000
- Service Platforms – NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

`edge-vlan`

Parameters

None

Example

```
nx9500-6C8809(config-profile-default-rfs4000-bridge-vlan-1)#edge-vlan
nx9500-6C8809(config-profile-default-rfs4000-bridge-vlan-1)#
```

Related Commands

|                             |                             |
|-----------------------------|-----------------------------|
| <code>no</code> on page 909 | Disables the edge VLAN mode |
|-----------------------------|-----------------------------|

firewall

[bridge-vlan-mode commands](#) on page 888

Enables IPv4 firewall on this Bridge VLAN. This feature is enabled by default.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

**firewall**

Parameters

None

Example

```
nx9500-6c8809(config-profile-default-rfs4000-bridge-vlan-1)#firewall
nx9500-6c8809(config-profile-default-rfs4000-bridge-vlan-1)#
```

Related Commands

|                                |                                                 |
|--------------------------------|-------------------------------------------------|
| <a href="#">no</a> on page 909 | Disables firewall on this bridge VLAN interface |
|--------------------------------|-------------------------------------------------|

http-analyze

[bridge-vlan-mode commands](#) on page 888

Enables the analysis of URLs and data traffic on this Bridge VLAN. When enabled, URLs and data are forwarded to the controller running the HTTP analytics engine.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

**http-analyze** {*filter* [*images*/*post*/*query-string*]}

Parameters

**http-analyze** {*filter* [*images*/*post*/*query-string*]}

|                                   |                                                                                                                                                                                                                                                                                   |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>http-analyze</b>               | Enables URL and HTTP data analysis. Optionally use the filter keyword to filter out specific URLs                                                                                                                                                                                 |
| <b>filter</b>                     |                                                                                                                                                                                                                                                                                   |
| <b>[images post query-string]</b> | <ul style="list-style-type: none"><li>• filter - Optional. Filters out specific URLs</li><li>• images - Filters out URLs referring to images</li><li>• post - Filters out URLs referring to POSTs</li><li>• query-string - Filters out query strings received from URLs</li></ul> |

## Example

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-bridge-vlan-4)#http-analyze filter images

rfs4000-229D58(config-device 00-23-68-22-9D-58-bridge-vlan-4)#show context
 bridge vlan 4
 http-analyze filter images
rfs4000-229D58(config-device 00-23-68-22-9D-58-bridge-vlan-4)#
```

## Related Commands

|                                |                                                                                          |
|--------------------------------|------------------------------------------------------------------------------------------|
| <a href="#">no</a> on page 909 | Disables forwarding of URLs and data to the controller running the HTTP analytics engine |
|--------------------------------|------------------------------------------------------------------------------------------|

ip

[bridge-vlan-mode commands](#) on page 888

Configures this Bridge VLAN's IP components

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

## Syntax

```
ip [arp|dhcp|igmp]
```

```
ip [arp|dhcp] trust
```

```
ip igmp snooping {fast-leave|forward-unknown-multicast|last-member-query-count| mrouter|querier}
```

```
ip igmp snooping {fast-leave|forward-unknown-multicast|last-member-query-count <1-7>}
```

```
ip igmp snooping {mrouter [interface|learn]}
```

```
ip igmp snooping {mrouter [interface <INTERFACE-LIST>|learn pim-dvmrp]}
```

```
ip igmp snooping {querier} {address|max-response-time|timer|version}
```

```
ip igmp snooping {querier} {address <IP>|max-response-time <1-25>|timer expiry <60-300>|version <1-3>}
```

## Parameters

```
ip [arp|dhcp] trust
```

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ip</b>         | Configures the VLAN bridge IP parameters                                                                                                                                                                                                                                                                                                                                                                             |
| <b>arp trust</b>  | Configures the ARP trust parameter. Trusted ARP packets are used to update the DHCP snoop table to prevent IP spoof and arp-cache poisoning attacks. This option is disabled by default. <ul style="list-style-type: none"> <li>• trust – Trusts ARP responses on the VLAN bridge</li> </ul>                                                                                                                         |
| <b>dhcp trust</b> | Configures the DHCP trust parameter. Uses DHCP packets, from a DHCP server, as trusted and permissible within the access point, wireless controller, or service platform managed network. DHCP packets are used to update the DHCP snoop table to prevent IP spoof attacks. This feature is enabled by default. <ul style="list-style-type: none"> <li>• trust – Trusts DHCP responses on the VLAN bridge</li> </ul> |

```
ip igmp snooping {fast-leave|forward-unknown-multicast|last-member-query-count <1-7>}
```

|                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ip</b>                                  | Configures the VLAN bridge IP parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>igmp snooping</b>                       | Configures Internet Group Management Protocol (IGMP) snooping parameters. IGMP snooping is enabled by default. IGMP establishes and maintains multicast group memberships for interested members. Multicasting allows a networked device to listen to IGMP network traffic and forward IGMP multicast packets to radios on which the interested hosts are connected. The device also maintains a map of the links that require multicast streams, there by reducing unnecessary flooding of the network with multicast traffic.                                                                                                |
| <b>fast-leave</b>                          | Optional. Enables fast leave processing. When enabled, layer 2 LAN interfaces are removed from the IGMP snooping forwarding table entry without initially sending IGMP group-specific queries to the interface. When receiving a group specific IGMPv2 leave message, IGMP snooping removes the interface from the Layer 2 forwarding table entry for that multicast group, unless a multicast router was learned on the port. Fast-leave processing enhances bandwidth management for all hosts on the network. This option is disabled by default. This feature is supported only on the AP7502, AP8533 model access points. |
| <b>forward-unknown-multicast</b>           | Optional. Enables forwarding of multicast packets from unregistered multicast groups. If disabled, the unknown multicast forward feature is also disabled for individual VLANs. This option is enabled by default.                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>last-member-query-count &lt;1-7&gt;</b> | Optional. Configures the last member query count used in determining the number of group-specific queries sent before removing the snoop entry <ul style="list-style-type: none"> <li>• &lt;1-7&gt; – Specify the count from 1 - 7. The default value is 2.</li> </ul>                                                                                                                                                                                                                                                                                                                                                         |

```
ip igmp snooping {mrouter [interface <INTERFACE-LIST>|learn pim-dvmrp]}
```

|                      |                                                      |
|----------------------|------------------------------------------------------|
| <b>ip</b>            | Configures the VLAN bridge IP parameters             |
| <b>igmp snooping</b> | Configures the IGMP snooping parameters              |
| <b>mrouter</b>       | Optional. Configures the multicast router parameters |

|                                                        |                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>interface</b><br><b>&lt;INTERFACE-<br/>LIST&gt;</b> | Configures the multicast router interfaces. This option is disabled by default. <ul style="list-style-type: none"> <li>• &lt;INTERFACE-LIST&gt; - Specify a comma-separated list of interface names.</li> </ul>                                                                 |
| <b>learn pim-dvmrp</b>                                 | Configures the multicast router learning protocols. This option is disabled by default. <ul style="list-style-type: none"> <li>• pim-dvmrp - Enables Protocol-Independent Multicast (PIM) and Distance-Vector Multicast Routing Protocol (DVMRP) snooping of packets</li> </ul> |

```
ip igmp snooping {querier} {address <IP>|max-response-time <1-25>| timer expiry <60-300>|
version <1-3>}
```

|                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ip</b>                             | Configures the VLAN bridge IP parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>igmp snooping</b>                  | Configures the IGMP snooping parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>querier</b>                        | Optional. Configures the IGMP querier parameters. This option is disabled by default. Enables IGMP querier. IGMP snoop querier keeps host memberships alive. It is primarily used in a network where there is a multicast streaming server and hosts subscribed to the server and no IGMP querier present. The access point, wireless controller, or service platform performs the IGMP querier role. An IGMP querier sends out periodic IGMP query packets. Interested hosts reply with an IGMP report packet. IGMP snooping is only conducted on wireless radios. IGMP multicast packets are flooded on wired ports. IGMP multicast packet are not flooded on the wired port. IGMP membership is also learnt on it and only if present, then it is forwarded on that port. |
| <b>address &lt;IP&gt;</b>             | Optional. Configures the IGMP querier source IP address. This address is used as the default VLAN querier IP address. <ul style="list-style-type: none"> <li>• &lt;IP&gt; - Specify the IGMP querier source IP address.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>max-response-time &lt;1-25&gt;</b> | Optional. Configures the IGMP querier maximum response time. This option is disabled by default. <ul style="list-style-type: none"> <li>• &lt;1-25&gt; - Specify the maximum response time from 1 - 25 seconds.</li> </ul> <p>The access point, wireless controller, or service platform forwards multicast packets only to radios present in the snooping table. IGMP reports from wired ports are forwarded to the multicast router ports.</p> <p>If no reports are received from a radio, it is removed from the snooping table. The radio then stops receiving multicast packets.</p>                                                                                                                                                                                    |
| <b>timer expiry &lt;60-300&gt;</b>    | Optional. Configures the IGMP querier expiry time. The value specified is used as the timeout interval for other querier resources. This option is disabled by default. <ul style="list-style-type: none"> <li>• expiry - Configures the IGMP querier timeout <ul style="list-style-type: none"> <li>• &lt;60-300&gt; - Specify the IGMP querier timeout from 60 - 300 seconds.</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                       |
| <b>version &lt;1-3&gt;</b>            | Optional. Configures the IGMP version. This option is disabled by default. <ul style="list-style-type: none"> <li>• &lt;1-3&gt; - Specify the IGMP version. The versions are 1- 3.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

#### Example

```
nx9500-6C8809(config-profile-default-rfs4000-bridge-vlan-1)#ip arp trust

nx9500-6C8809(config-profile-default-rfs4000-bridge-vlan-1)#ip dhcp trust

nx9500-6C8809(config-profile-default-rfs4000-bridge-vlan-1)#ip igmp snooping mrouter
interface ge1 ge2

nx9500-6C8809(config-profile-default-rfs4000-bridge-vlan-1)#ip igmp snooping mrouter learn
pim-dvmrp

nx9500-6C8809(config-profile-default-rfs4000-bridge-vlan-1)#ip igmp snooping querier max-
```

```

response-time 24

nx9500-6C8809(config-profile-default-rfs4000-bridge-vlan-1)#ip igmp snooping querier timer
expiry 100

nx9500-6C8809(config-profile-default-rfs4000-bridge-vlan-1)#ip igmp snooping querier
version 2

nx9500-6C8809(config-profile-default-rfs4000-bridge-vlan-1)#show context
bridge vlan 1
 description "This is a description for the bridged VLAN"
 ip arp trust
 ip dhcp trust
 ip igmp snooping
 ip igmp snooping querier
 ip igmp snooping querier version 2
 ip igmp snooping querier max-response-time 24
 ip igmp snooping querier timer expiry 100
 ip igmp snooping mrouter interface ge2 ge1
nx9500-6C8809(config-profile-default-rfs4000-bridge-vlan-1)#

```

#### Related Commands

|                |                                                         |
|----------------|---------------------------------------------------------|
| no on page 909 | Disables or reverts the VLAN Ethernet bridge parameters |
|----------------|---------------------------------------------------------|

ipv6

[bridge-vlan-mode commands](#) on page 888

Configures this Bridge VLAN's IPv6 components

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ipv6 [dhcpv6|firewall|mld|nd]
```

```
ipv6 dhcpv6 trust
```

```
ipv6 firewall
```

```
ipv6 mld snooping {forward-unknown-multicast|mrouter|querier}
```

```
ipv6 mld snooping {forward-unknown-multicast}
```

```
ipv6 mld snooping {mrouter [interface|learn]}
```

```
ipv6 mld snooping {mrouter [interface <INTERFACE-LIST>|learn pim-dvmrp]}
```

```
ipv6 mld snooping {querier} {max-response-time|timer|version}
```

```
ipv6 mld snooping {querier} {max-response-time <1-25000>|timer expiry
<60-300>| version <1-2>}
```

## ipv6 nd raguard

### Parameters

ipv6 dhcpv6 trust

|                     |                                                                                                                                                                                                                                              |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipv6</b>         | Configures the VLAN bridge IPv6 parameters                                                                                                                                                                                                   |
| <b>dhcpv6 trust</b> | Enables the DHCPv6 trust option. When enabled all DHCPv6 responses are trusted on this bridge VLAN. This option is enabled by default. <ul style="list-style-type: none"><li>• trust - Trusts DHCPv6 responses on this bridge VLAN</li></ul> |

## ipv6 firewall

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipv6</b>     | Configures the VLAN bridge IPv6 parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>firewall</b> | Enables IPv6 firewall on this bridge VLAN. This option is enabled by default. Devices utilizing IPv6 addressing require firewall protection unique to IPv6 traffic. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery (ND) protocol via ICMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters. Routers respond to such a request with a router advertisement (RA) packet that contains Internet layer configuration parameters. |

## ipv6 mld snooping {forward-unknown-multicast}

|                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipv6</b>                      | Configures the VLAN bridge IPv6 parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>mld snooping</b>              | Configures Multicast Listener Discovery Protocol (MLD) snooping parameters. MLD snooping enables a access point, wireless controller, or service platform to examine MLD packets and make forwarding decisions based on the content. MLD is used by IPv6 devices to discover devices wanting to receive multicast packets destined for specific multicast addresses. MLD uses multicast listener queries and multicast listener reports to identify which multicast addresses have listeners and join multicast groups. MLD snooping caps the flooding of IPv6 multicast traffic on controller, service platform or access point VLANs. When enabled, MLD messages between hosts and multicast routers are examined to identify the hosts receiving multicast group traffic. The access point, wireless controller, or service platform forward multicast traffic only to those interfaces connected to interested receivers instead of flooding traffic to all interfaces. This option is enabled by default. |
| <b>forward-unknown-multicast</b> | Optional. Enables forwarding of multicast packets from unregistered multicast groups. If disabled, the unknown multicast forward feature is also disabled for individual VLANs. This option is enabled by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## ipv6 mld snooping {mrouter [interface <INTERFACE-LIST>|learn pim-dvmrp]}

|                     |                                                                                                      |
|---------------------|------------------------------------------------------------------------------------------------------|
| <b>ipv6</b>         | Configures the VLAN bridge IPv6 parameters                                                           |
| <b>mld snooping</b> | Configures MLD snooping parameters. This option is enabled by default.                               |
| <b>mrouter</b>      | Optional. Configures the multicast router parameters, such as interfaces and learning protocol used. |

|                                                        |                                                                                                                                                                                                                 |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>interface</b><br><b>&lt;INTERFACE-<br/>LIST&gt;</b> | Configures the multicast router interfaces. This option is disabled by default. <ul style="list-style-type: none"> <li>• &lt;INTERFACE-LIST&gt; - Specify a comma-separated list of interface names.</li> </ul> |
| <b>learn pim-dvmrp</b>                                 | Configures the multicast router learning protocols. This option is disabled by default. <ul style="list-style-type: none"> <li>• pim-dvmrp - Enables PIM and DVMRP snooping of packets</li> </ul>               |

```
ipv6 mld snooping {querier} {max-response-time <1-25000>|timer expiry <60-300>| version <1-2>}
```

|                                          |                                                                                                                                                                                                                                                                                    |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipv6</b>                              | Configures the VLAN bridge IPv6 parameters                                                                                                                                                                                                                                         |
| <b>mld snooping</b>                      | Configures IPv6 MLD snooping parameters. This option is disabled by default.                                                                                                                                                                                                       |
| <b>querier</b>                           | Optional. Enables and configures the MLD querier parameters. When enabled, the device (access point, wireless controller, and service platform) sends query messages to discover which network devices are members of a given multicast group. This option is disabled by default. |
| <b>max-response-time &lt;1-25000&gt;</b> | Optional. Configures the IPv6 MLD querier's maximum response time. This option is disabled by default. <ul style="list-style-type: none"> <li>• &lt;1-25000&gt; - Specify the maximum response time from 1 - 25000 milliseconds.</li> </ul>                                        |
| <b>timer expiry &lt;60-300&gt;</b>       | Optional. Configures the IPv6 MLD other querier's timeout. This option is disabled by default. <ul style="list-style-type: none"> <li>• &lt;60-300&gt; - Specify the MLD other querier's timeout from 60 - 300 seconds.</li> </ul>                                                 |
| <b>version &lt;1-2&gt;</b>               | Optional. Configures the IPv6 MLD querier version. This option is disabled by default. <ul style="list-style-type: none"> <li>• &lt;1-2&gt; - Specify the MLD version. The versions are 1- 2.</li> </ul>                                                                           |

```
ipv6 nd rguard
```

|                  |                                                                                                              |
|------------------|--------------------------------------------------------------------------------------------------------------|
| <b>ipv6</b>      | Configures the VLAN bridge IPv6 parameters                                                                   |
| <b>nd rguard</b> | Allows router advertisement (RA) or ICMPv6 redirects on this VLAN bridge. This option is enabled by default. |

#### Example

```
rfs7000-37FABE(config-profile test-bridge-vlan-2)#ipv6 dhcpv6 trust

rfs7000-37FABE(config-profile test-bridge-vlan-2)#ipv6 firewall

rfs7000-37FABE(config-profile test-bridge-vlan-2)#ipv6 mld snooping forward-unknown-multicast

rfs7000-37FABE(config-profile test-bridge-vlan-2)#ipv6 mld snooping mrouter interface ge1 ge2

rfs7000-37FABE(config-profile test-bridge-vlan-2)#ipv6 mld snooping mrouter learn pim-dvmrp

rfs7000-37FABE(config-profile test-bridge-vlan-2)#ipv6 mld snooping querier max-response-time 20000

rfs7000-37FABE(config-profile test-bridge-vlan-2)#ipv6 mld snooping querier timer expiry 200

rfs7000-37FABE(config-profile test-bridge-vlan-2)#ipv6 mld snooping querier version 2

rfs7000-37FABE(config-profile test-bridge-vlan-2)#show context
```



```

bridge vlan 2
 ip igmp snooping
 ip igmp snooping querier
 ipv6 mld snooping
 ipv6 mld snooping querier
 ipv6 mld snooping mrouter interface ge2 ge1
 ipv6 mld snooping querier version 2
 ipv6 mld snooping querier max-response-time 20000
 ipv6 mld snooping querier timer expiry 200
 rfs7000-37FABE(config-profile test-bridge-vlan-2)#

```

#### Related Commands

|                                |                                                              |
|--------------------------------|--------------------------------------------------------------|
| <a href="#">no</a> on page 909 | Disables or reverts the VLAN Ethernet bridge IPv6 parameters |
|--------------------------------|--------------------------------------------------------------|

## l2-tunnel-broadcast-optimization

[bridge-vlan-mode commands](#) on page 888

Enables broadcast optimization on this bridge VLAN. L2 Tunnel Broadcast Optimization prevents flooding of ARP packets over the virtual interface. Based on the learned information, ARP packets are filtered at the wireless controller level.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
l2-tunnel-broadcast-optimization
```

#### Parameters

None

#### Example

```

nx9500-6C8809(config-profile-default-rfs4000-bridge-vlan-1)#l2-tunnel-broadcast
-optimization

```

```

nx9500-6C8809(config-profile-default-rfs4000-bridge-vlan-1)#show context

```

```

bridge vlan 1
 description "This is a description for the bridged VLAN"
 l2-tunnel-broadcast-optimization
 bridging-mode isolated-tunnel
 ip arp trust
 ip dhcp trust
 ip igmp snooping
 ip igmp snooping querier
 ip igmp snooping mrouter interface ge2 ge1
 ip igmp snooping querier version 2
 ip igmp snooping querier max-response-time 24
 ip igmp snooping querier timer expiry 100
 nx9500-6C8809(config-profile-default-rfs4000-bridge-vlan-1)#

```

#### Related Commands

|                                |                                           |
|--------------------------------|-------------------------------------------|
| <a href="#">no</a> on page 909 | Disables L2 tunnel broadcast optimization |
|--------------------------------|-------------------------------------------|

## l2-tunnel-forward-additional-packet-types

[bridge-vlan-mode commands](#) on page 888

Enables forwarding of Wireless Network Management Protocol (WNMP) packets across L2 tunnels. Under normal circumstances, if L2 tunnel broadcast optimization is enabled, WNMP packets are not forwarded across the L2 tunnels. Use this option to enable the forwarding of only WNMP packets.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
l2-tunnel-forward-additional-packet-types wnmp
```

Parameters

None

Example

```
nx9500-6C8809(config-profile testNX9000-bridge-vlan-1)#l2-tunnel-forward-additional-packet-types wnmp
```

```
nx9500-6C8809(config-profile testNX9000-bridge-vlan-1)#show context
bridge vlan 1
 l2-tunnel-broadcast-optimization
 l2-tunnel-forward-additional-packet-types wnmp
 ip igmp snooping
 ip igmp snooping querier
 ipv6 mld snooping
 ipv6 mld snooping querier
nx9500-6C8809(config-profile testNX9000-bridge-vlan-1)#
```

Related Commands

|                                |                                                  |
|--------------------------------|--------------------------------------------------|
| <a href="#">no</a> on page 909 | Disables WNMP packet forwarding across L2 tunnel |
|--------------------------------|--------------------------------------------------|

## mac-auth

[bridge-vlan-mode commands](#) on page 888

Enables source MAC authentication for Extended VLAN and tunneled traffic (MiNT and L2TPv3) on this bridge VLAN. When enabled, it provides fast path authentications of clients, whose captive portal session has expired.

Supported in the following platforms:

- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
mac-auth {attempts <1-5>/throttle <0-255>}
```

## Parameters

`mac-auth {attempts <1-5>|throttle <0-255>}`

|                               |                                                                                                                                                                                                                                              |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mac-auth</b>               | Enables MAC Authentication                                                                                                                                                                                                                   |
| <b>attempts &lt;1-5&gt;</b>   | Optional. Configures the maximum number of retries allowed for MAC authentication requests. <ul style="list-style-type: none"><li>• &lt;1-5&gt; - Specify the maximum allowed authentication retries from 1 - 5. The default is 3.</li></ul> |
| <b>throttle &lt;0-255&gt;</b> | Optional. Configures the throttle value for MAC authentication requests <ul style="list-style-type: none"><li>• &lt;0-255&gt; - Specify the MAC authentication request throttle value from 0 -255. The default is 64.</li></ul>              |

## Usage Guidelines Applying AAA Policy for MAC Authentication

To enable MAC authentication,

- Create an AAA policy.

```
nx9500-6C8809(config)#aaa-policy MAC-Auth
```

- Use the AAA policy on the device for MAC Authentication.

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#mac-auth use aaa-policy MAC-Auth
```

- In the bridge VLAN context, enable MAC Authentication,

```
nx9500-6C8809(config-device B4-C7-99-6C-88-09-bridge-vlan-20)#mac-auth
```

- Optionally, configure the following MAC Authentication parameters. If not specified, default values are applied.

```
nx9500-6C8809(config-device B4-C7-99-6C-88-09-bridge-vlan-20)#mac-auth attempts 2
```

```
nx9500-6C8809(config-device B4-C7-99-6C-88-09-bridge-vlan-20)#mac-auth throttle 100
```

## Usage Guidelines Enabling Fall-back Captive Portal Authentication

To enable fall-back captive-portal authentication on the bridge VLAN,

- apply a captive-portal policy to the bridge VLAN.

```
nx9500-6C8809(config-device B4-C7-99-6C-88-09-bridge-vlan-20)#use captive-portal test
```

- enable captive-portal authentication as the fall-back authentication mode.

```
nx9500-6C8809(config-device B4-C7-99-6C-88-09-bridge-vlan-20)#captive-portal-enforcement
fall-back
```

## Example

```
nx9500-6C8809(config-profile testNX9000-bridge-vlan-20)#mac-auth attempts 2
```

```
nx9500-6C8809(config-profile testNX9000-bridge-vlan-20)#mac-auth throttle 80
```

```
nx9500-6C8809(config-profile testNX9000-bridge-vlan-20)#show context
```

```
bridge vlan 20
 mac-auth attempts 2
 mac-auth throttle 80
 ip igmp snooping
 ip igmp snooping querier
```

```
ipv6 mld snooping
ipv6 mld snooping querier
nx9500-6C8809(config-profile testNX9000-bridge-vlan-20)#
```

#### Related Commands

|                                |                                                                                        |
|--------------------------------|----------------------------------------------------------------------------------------|
| <a href="#">no</a> on page 909 | Disables MAC authentication for Extended VLAN and Tunneled traffic on this bridge VLAN |
|--------------------------------|----------------------------------------------------------------------------------------|

name

[bridge-vlan-mode commands](#) on page 888

Configures a name for this Bridge VLAN. This name uniquely identifies the bridge-vlan interface, and is forwarded to the EGuest server along with configuration details.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
name <NAME>
```

#### Parameters

```
name <NAME>
```

|                          |                                                                                                                                                                       |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>name &lt;NAME&gt;</b> | Provide a name for this Bridge VLAN, uniquely identifying it from other Bridge VLAN interfaces with similar configurations. It should exceed 32 characters in length. |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
nx9500-6C8809(config-profile testNX5500-bridge-vlan-200)#name InterLabs1-2
```

```
nx9500-6C8809(config-profile testNX5500-bridge-vlan-200)#show context
bridge vlan 200
 name InterLabs1-2
 ip igmp snooping
 ip igmp snooping querier
 ipv6 mld snooping
 ipv6 mld snooping querier
nx9500-6C8809(config-profile testNX5500-bridge-vlan-200)#
```

#### Related Commands

|                                |                                                       |
|--------------------------------|-------------------------------------------------------|
| <a href="#">no</a> on page 909 | Removes or modifies this Bridge VLANs configured name |
|--------------------------------|-------------------------------------------------------|

registration

[bridge-vlan-mode commands](#) on page 888

Enables forwarding of bridge-vlan information (such as, name and vlan) to the ExtremeGuest (EGuest) server. The EGuest server updates its WLAN information collection with the received wired-network information.



#### Note

Ensure that the bridge-vlan interface has a name that uniquely identifies it from other bridge-vlan interfaces with similar configurations. For more information, see [name](#) on page 904.

Captive-portal Web pages for wired clients are hosted on the gateway controller's bridge-vlan interface. By updating the EGuest server with bridge-vlan information, you enable the EGuest server to apply of captive-portal's Splash templates to the bridge-vlan interface.

This command also configures the external guest registration and validation server details. If using an external server to perform wired client registration, authentication and accounting, use this command to configure the external server's IP address/hostname. When configured, the gateway controller forwards guest registration requests to the specified registration server. In case of EGuest deployment, this external resource should point to the EGuest server.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
registration [device|device-OTP|external|user]
registration [device|device-otp|user] group-name <RADIUS-GROUP-NAME>
expiry-time <1-43800>
registration external follow-aaa send-mode [http|https|udp]
```

#### Parameters

```
registration [device|device-OTP|user] group-name <RAD-GROUP-NAME> {expiry-time <1-43800>}
```

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>registration</b>                 | Enables wired guest-user registration and validation. This option is disabled by default. Use to configure registration and validation parameters for wired captive-portal clients. Specify the client registration mode used. If using an external resource as authenticating server, use this command to point to the external resource.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>[device   device-OTP   user]</b> | <p>Configures the mode used to register wired clients on this bridge-vlan interface. The options are: device, user, and device-OTP.</p> <ul style="list-style-type: none"><li>• device-OTP – Registers device by its MAC address. During registration the user, provides e-mail address or mobile number, and an OTP (one-time-passcode) is sent to the registered e-mail id or mobile number to complete registration.</li><li>• device – Registers device by its MAC address, and allows access to already registered clients.</li></ul> <p><b>Note:</b> If using the above two options, ensure MAC authentication is enabled on the bridge-vlan interface.</p> <ul style="list-style-type: none"><li>• user – Registers guest users using one of the following options: e-mail address, mobile-number, or member-id.</li></ul> <p>If using any one of the above modes of registration, specify the RADIUS group to which the registered device or user is to be assigned post authentication.</p> |

|                                                    |                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>group-name</b><br><b>&lt;RAD-GROUP-NAME&gt;</b> | Configures the RADIUS group name in which registered users are placed. When left blank, users are not associated with a RADIUS group. <ul style="list-style-type: none"> <li>• &lt;RAD-GROUP-NAME&gt; - Specify the RADIUS group name (should not exceed 64 characters).</li> </ul>                                   |
| <b>expiry-time</b><br><b>&lt;1-43800&gt;</b>       | Optional. Configures the duration in hours, or which registered MAC addresses are retained. Once this duration is over, registered MAC addresses expire and need to be re-entered. <ul style="list-style-type: none"> <li>• &lt;1-43800&gt; - Specify a value from 1 - 43800 hrs. The default is 1500 hrs.</li> </ul> |

```
registration external follow-aaa send-mode [http|https|udp]
```

|                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>registration</b>                          | Enables wired guest-user registration and validation. This option is disabled by default. Use to configure registration and validation parameters for wired captive-portal clients. Specify the client registration mode used. If using an external resource as authenticating server, use this command to point to the external resource.                                                                                                                                                                                                                                                                                                                       |
| <b>external</b>                              | Specifies that the wired client registration is handled by an external resource. Registration requests are forwarded to the external registration server by the captive-portal gateway controller.                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>follow-aaa</b>                            | Uses an AAA policy to point to the guest registration, authentication, and accounting server. When used, guest registration is handled by the RADIUS server specified in the AAA policy. This is the AAA policy used in the captive-portal applied on the bridge-vlan interface.<br>In case of EGuest deployment, in the AAA policy, the RADIUS authentication and accounting server configuration should point to the EGuest server. The use of 'follow-aaa' option is recommended in EGuest replica-set deployments.<br>For more information on enabling the EGuest server, see <a href="#">eguest-server (VX9000 only)</a> on page 990 (profile config mode). |
| <b>send-mode</b><br><b>[https https udp]</b> | Specifies the protocol used to forward registration requests to the external AAA policy server. The options are: <ul style="list-style-type: none"> <li>• HTTPS - Sends registration requests as HTTPS packet</li> <li>• HTTP - Sends registration requests as HTTP packet</li> <li>• UDP - Sends registration requests as UDP packet. This is the default setting.</li> </ul>                                                                                                                                                                                                                                                                                   |

#### Example

```
nx9500-6C8809(config-profile testNX9500-bridge-vlan-20)#registration device
group-name test expiry-time 200
nx9500-6C8809(config-profile testNX9500-bridge-vlan-20)#registration external
follow-aaa send-mode https
nx9500-6C8809(config-profile testNX9500-bridge-vlan-20)#show context
bridge vlan 20
 registration device group-name test expiry-time 200
 registration external follow-aaa send-mode https
 ip igmp snooping
 ip igmp snooping querier
 ipv6 mld snooping
 ipv6 mld snooping querier
nx9500-6C8809(config-profile testNX9500-bridge-vlan-20)#
```

#### Related Commands

|                       |                                                                                   |
|-----------------------|-----------------------------------------------------------------------------------|
| <b>no</b> on page 909 | Disables self-registration of captive-portal users on this bridge-vlan interface. |
|-----------------------|-----------------------------------------------------------------------------------|

stateful-packet-inspection-l2

[bridge-vlan-mode commands](#) on page 888

Enables a stateful packet inspection (SPI) at the layer 2 firewall. SPI, also referred to as dynamic packet filtering, is a security feature that tracks the operating state and characteristics of network connections traversing it. It distinguishes legitimate packets for different types of connections, and only allows packets matching a known active connection to pass.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
stateful-packet-inspection-12
```

Parameters

None

Example

```
nx9500-6C8809(config-profile-default-rfs4000-bridge-vlan-1)#stateful-packet-inspection-12
nx9500-6C8809(config-profile-default-rfs4000-bridge-vlan-1)#
```

Related Commands

|                                |                                                             |
|--------------------------------|-------------------------------------------------------------|
| <a href="#">no</a> on page 909 | Disables stateful packet inspection at the layer 2 firewall |
|--------------------------------|-------------------------------------------------------------|

tunnel

[bridge-vlan-mode commands](#) on page 888

Enables tunneling of unicast messages, to unknown MAC destinations, on the selected VLAN bridge

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
tunnel [rate-limit|unknown-unicast]
```

```
tunnel rate-limit level2 rate <50-1000000> max-burst-size <2-1024> {red-threshold [background <0-100>|best-effort <0-100>|video <0-100>|voice <0-100>]}
tunnel unknown-unicast
```

Parameters

```
tunnel rate-limit level2 rate <50-1000000> max-burst-size <2-1024> {red-threshold [background <0-100>|best-effort <0-100>|video <0-100>|voice <0-100>]}
```

**tunnel rate-limit level2 rate <50-1000000> max-burst-size <2-1024>**

- Configures a rate-limit parameters (max-burst-size and rate) for tunneled VLAN traffic over level 2 MiNT links
- rate - Optional. Configures the data rate, in kilobits per second, for the incoming and outgoing extended VLAN traffic tunneled over MiNT level 2 links
  - <50-1000000> - Specify a value from 50 - 1000000 Kbps. The default is 5000 Kbps.
  - max-burst-size - Optional. Configures the maximum burst size
  - <2-1024> - Specify the maximum burst size from 2 - 1024 kbytes. The default is 320 kbytes.

After specifying the max-burst-size, optionally specify the red-threshold value for the different traffic types. The red-threshold is configured as a % of the specified max-burst-size.

- red-threshold - Optional. Configures the random early detection (red) threshold for the different traffic types
  - background - Configures the red-threshold for low priority traffic from 0 - 100. The default is 50% of the specified max-burst-size.
  - best-effort - Configures the red-threshold for normal priority traffic from 0 - 100. The default is 50% of the specified max-burst-size.
  - video - Configures the red-threshold for video traffic from 0 - 100. The default is 25% of the specified max-burst-size.
  - voice - Configures the red-threshold for voice traffic from 0 - 100. The default is 0% of the specified max-burst-size.

tunnel unknown-unicast

**tunnel unknown-unicast**

Enables tunneling of unicast packets destined for unknown MAC addresses

#### Example

```
nx9500-6C8809(config-profile TestAP81xx-bridge-vlan-1)#tunnel unknown-unicast
nx9500-6C8809(config-profile TestAP81xx-bridge-vlan-1)#no tunnel unknown-unicast
nx9500-6C8809(config-profile TestAP81xx-bridge-vlan-1)#show context
bridge vlan 1
 ip igmp snooping
 ip igmp snooping querier
 no tunnel unknown-unicast
nx9500-6C8809(config-profile TestAP81xx-bridge-vlan-1)#
```

#### Related Commands

**no** on page 909

Disables tunneling of unicast messages, to unknown MAC destinations, on the selected VLAN bridge

tunnel-over-level2

[bridge-vlan-mode commands](#) on page 888

Enables extended VLAN (tunneled VLAN) traffic over level 2 MiNT links. This option is disabled by default.

Supported in the following platforms:



- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

`tunnel-over-level2`

#### Parameters

None

#### Example

```
rfs4000-229D58(config-profile testRFS4000-bridge-vlan-1)#tunnel-over-level2
```

```
rfs4000-229D58(config-profile testRFS4000-bridge-vlan-1)#show context
bridge vlan 1
 description "This is a description for the bridged VLAN"
 12-tunnel-broadcast-optimization
 bridging-mode isolated-tunnel
 tunnel-over-level2
 ip arp trust
 ip dhcp trust
 ip igmp snooping
 ip igmp snooping querier
rfs4000-229D58(config-profile testRFS4000-bridge-vlan-1)#
```

#### Related Commands

|                                |                                                        |
|--------------------------------|--------------------------------------------------------|
| <a href="#">no</a> on page 909 | Disables extended VLAN traffic over level 2 MiNT links |
|--------------------------------|--------------------------------------------------------|

no

[bridge-vlan-mode commands](#) on page 888

Negates a command or reverts settings to their default. The no command, when used in the bridge VLAN mode, negates the VLAN bridge settings or reverts them to their default.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
no [bridging-mode | captive-portal | captive-portal-enforcement | description |
edge-vlan | firewall | http-analyze | ip | ipv6 | 12-tunnel-broadcast-optimization |
12-tunnel-forward-additional-packet-types | mac-auth | name | registration |
stateful-packet-inspection-12 | tunnel | tunnel-over-level2 | use]
```

```
no [bridging-mode | captive-portal-enforcement | description | edge-vlan |
firewall | 12-tunnel-broadcast-optimization | 12-tunnel-forward-additional-
packet-types | mac-auth | name | stateful-packet-inspection-12 | tunnel-over-
level2]
```

```

no captive-portal [ip-snooping|ipv6-snooping] subnet <IPv4/M|IPv6/M>
{excluded-address <IPv4/IPv6>}

no http-analyze {filter [images/post/query-string]}

no ip [arp|dhcp|igmp]

no ip [arp|dhcp] trust
no ip igmp snooping {fast-leave/forward-unknown-multicast/last-member-
query-count/mrouter/querier}
no ip igmp snooping {forward-unknown-multicast}
no ip igmp snooping {mrouter [interface <INTERFACE-LIST>|learn pin-
dvmrp]}
no ip igmp snooping {querier} {address/max-response-time/timer expiry/
version}

no ipv6 [dhcpv6|firewall|mld|nd]

no ipv6 dhcpv6 trust
no ipv6 firewall
no ipv6 mld snooping {forward-unknown-multicast}
no ipv6 mld snooping {mrouter [interface <INTERFACE-LIST>|learn pin-
dvmrp]}
no ipv6 mld snooping {querier} {max-response-time/timer expiry/version}
no ipv6 nd rguard

no registration {external}

no tunnel [rate-limit level2|unknown-unicast]

no use [application-policy|captive-portal|ip-access-list|ipv6-access-
list| mac-access-list|url-list] tunnel out

Parameters
no <PARAMETERS>

```

|                                                                                                           |
|-----------------------------------------------------------------------------------------------------------|
| <b>no &lt;PARAMETERS&gt;</b> Resets or reverts this bridge VLAN's settings based on the parameters passed |
|-----------------------------------------------------------------------------------------------------------|

#### Example

The following example displays bridge VLAN 20 settings before the 'no' commands are executed:

```

nx9500-6C8809(config-profile testNX9500-bridge-vlan-20)#show context
bridge vlan 20
 ip igmp snooping
 ip igmp snooping querier
 ipv6 mld snooping
 ipv6 mld snooping querier
nx9500-6C8809(config-profile testNX9500-bridge-vlan-20)#

nx9500-6C8809(config-profile testNX9500-bridge-vlan-20)#no ip igmp snooping
nx9500-6C8809(config-profile testNX9500-bridge-vlan-20)#no ipv6 mld snooping

```

The following example displays bridge VLAN 20 settings after the 'no' commands are executed:

```
nx9500-6C8809(config-profile testNX9500-bridge-vlan-20)#show context
 bridge vlan 20
 no ip igmp snooping
 ip igmp snooping querier
 no ipv6 mld snooping
 ipv6 mld snooping querier
nx9500-6C8809(config-profile testNX9500-bridge-vlan-20)#

nx9500-6C8809(config-profile TestProfileNX9500-bridge-vlan-20)#show context
 bridge vlan 20
 mac-auth attempts 2
 mac-auth throttle 80
 ip igmp snooping
 ip igmp snooping querier
 ipv6 mld snooping
 ipv6 mld snooping querier

nx9500-6C8809(config-profile TestProfileNX9500-bridge-vlan-20)#

nx9500-6C8809(config-profile TestProfileNX9500-bridge-vlan-20)#no mac-auth

nx9500-6C8809(config-profile TestProfileNX9500-bridge-vlan-20)#show context
 bridge vlan 20
 ip igmp snooping
 ip igmp snooping querier
 ipv6 mld snooping
 ipv6 mld snooping querier
nx9500-6C8809(config-profile TestProfileNX9500-bridge-vlan-20)#
```

use

[bridge-vlan-mode commands](#) on page 888

Associates a captive-portal, access control list (IPv4, IPv6, or MAC), and/or a URL filter with this bridge VLAN

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
use [application-policy | captive-portal | ip-access-list | ipv6-access-list |
mac-access-list | url-filter]
```

```
use application-policy <APP-POLICY-NAME>
```

```
use captive-portal <CAPTIVE-PORTAL-NAME>
```

```
use [ip-access-list | ipv6-access-list | mac-access-list] tunnel out <IP/
ipv6/MAC-ACCESS-LIST-NAME>
```

```
use url-filter <URL-FILTER-NAME>
```

## Parameters

use application-policy <APP-POLICY-NAME>

|                                                       |                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>use application-policy &lt;APP-POLICY-NAME&gt;</b> | Enforces application detection on this VLAN bridge                                                                                                                                                                                                                                                                                     |
|                                                       | <ul style="list-style-type: none"><li>• &lt;APP-POLICY-NAME&gt; – Specify the application policy name (should be existing and configured).</li><li>• For more information on application definitions and application policy, see <a href="#">application</a> on page 258 and <a href="#">application-policy</a> on page 267.</li></ul> |

use captive-portal <CAPTIVE-PORTAL-NAME>

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>use captive-portal</b> | Applies an existing captive portal configuration to restrict access to the bridge VLAN configuration<br>A captive portal is an access policy for providing temporary and restrictive access using a standard Web browser. Captive portals provide authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the network. Once logged into the captive portal, additional terms and agreement, welcome, fail, and no-service pages provide the administrator with a number of options on captive portal screen flow and user appearance. |
|                           | <ul style="list-style-type: none"><li>• &lt;CAPTIVE-PORTAL-NAME&gt; – Specify the captive portal name.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

use [ip-access-list|ipv6-access-list|mac-access-list] tunnel out <IP/IPv6/MAC-ACCESS-LIST-NAME>

|                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>use</b>                                             | Sets this VLAN bridge policy to use an IPv4/IPv6 access list or a MAC access list                                                                                                                                                                                                                                                                                                                                                      |
| <b>ip-access-list</b>                                  | Associates a pre-configured IPv4 access list with this VLAN-bridge interface                                                                                                                                                                                                                                                                                                                                                           |
| <b>ipv6-access-list</b>                                | Associates a pre-configured IPv6 access list with this VLAN-bridge interface                                                                                                                                                                                                                                                                                                                                                           |
| <b>mac-access-list</b>                                 | Associates a pre-configured MAC access list with this VLAN- bridge interface                                                                                                                                                                                                                                                                                                                                                           |
| <b>tunnel out &lt;IP/IPv6/MAC-ACCESS-LIST-NAME&gt;</b> | The following keywords are common to the 'IPv4/IPv6 access list' and 'MAC access list' parameters: <ul style="list-style-type: none"><li>• tunnel – Applies IPv4/IPv6 access list or MAC access list to all packets going into the tunnel</li><li>• out – Applies IPv4/IPv6 access list or MAC access list to all outgoing packets</li></ul> <IP/IPv6/MAC-ACCESS-LIST-NAME> – Specify the IP/IPv6 access list or MAC access list name. |

use url-filter <URL-FILTER-NAME>

|                                |                                                                                                                              |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>use url-filter</b>          | Sets this VLAN bridge to use a URL filter                                                                                    |
| <b>&lt;URL-FILTER-NAME&gt;</b> | Specify the URL filter name. It should be existing and configured.<br>This option enforces URL filtering on the VLAN bridge. |

## Example

```
nx9500-6C8809(config-profile-default-rfs4000-bridge-vlan-1)#use mac-access-list tunnel out PERMIT-ARP-AND-IPv4
```

```
nx9500-6C8809(config-profile-default-rfs4000-bridge-vlan-1)#show context
bridge vlan 1
 ip igmp snooping
 ip igmp snooping querier
```

```
use mac-access-list tunnel out PERMIT-ARP-AND-IPv4
nx9500-6C8809(config-profile-default-rfs4000-bridge-vlan-1)#
```

### Related Commands

|                                |                                                   |
|--------------------------------|---------------------------------------------------|
| <a href="#">no</a> on page 909 | Disables or reverts VLAN Ethernet bridge settings |
|--------------------------------|---------------------------------------------------|

## *captive-portal*

[Profile Config Commands](#) on page 862

Configures captive portal advanced Web page uploads on this profile

A captive portal is a means of providing guests temporary and restrictive access to the controller managed wireless network. A captive portal provides secure authenticated controller access by capturing and re-directing a wireless user's Web browser session to a captive portal login page, where the user must enter valid credentials. Once the user is authenticated and logged into the controller managed network, additional agreement, welcome, and fail pages provide the administrator with options to control the captive portal's screen flow and user appearance.

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
captive-portal page-upload count <1-20>
```

### Parameters

```
captive-portal page-upload count <1-20>
```

|                           |                                                                                                                                                                                 |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>page-upload</b>        | Enables captive portal advanced Web page upload                                                                                                                                 |
| <b>count &lt;1-20&gt;</b> | Sets the maximum number of APs that can be uploaded concurrently <ul style="list-style-type: none"> <li>• &lt;1-20&gt; - Set a value from 1 - 20. The default is 10.</li> </ul> |

### Example

```
nx9500-6C8809(config-profile-testNX9500)#captive-portal page-upload count 15

nx9500-6C8809(config-profile-testNX9500)#show context include-factory | include
captive-portal
captive-portal page-upload count 15
no captive-portal-enforcement
no captive-portal-enforcement
no captive-portal-enforcement
no captive-portal-enforcement
no captive-portal-enforcement
no captive-portal-enforcement
service captive-portal-server connections-per-ip 3
nx9500-6C8809(config-profile-testNX9500)#
```



[Profile Config Commands](#) on page 862

Enables Cisco Discovery Protocol (CDP), a proprietary data link layer network protocol implemented in Cisco networking equipment and used to share network information amongst different vendor wireless devices

**Supported in the following platforms:**

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
cdp [holdtime|run|timer]
```

```
cdp [holdtime <10-1800>|run|timer <5-900>]
```

**Parameters**

```
cdp [holdtime <10-1800>|run|timer <5-900>]
```

|                                           |                                                                                                                                                                                                                        |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>holdtime</b><br><b>&lt;10-1800&gt;</b> | Specifies the holdtime after which transmitted packets are discarded<br><ul style="list-style-type: none"> <li>• &lt;10-1800&gt; - Specify a value from 10 - 1800 seconds. The default is 180 seconds.</li> </ul>      |
| <b>run</b>                                | Enables CDP sniffing and transmit globally. This feature is enabled by default.                                                                                                                                        |
| <b>timer &lt;5-900&gt;</b>                | Specifies the interval, in seconds, between successive CDP packet transmission<br><ul style="list-style-type: none"> <li>• &lt;5-900&gt; - Specify a value from 5 - 900 seconds. The default is 60 seconds.</li> </ul> |

**Example**

```
nx9500-6C8809(config profile-default-rfs4000)#cdp run
nx9500-6C8809(config profile-default-rfs4000)#cdp holdtime 1000
nx9500-6C8809(config profile-default-rfs4000)#cdp timer 900
nx9500-6C8809(config-profile-default-rfs4000)#show context
profile rfs4000 default-rfs4000
 bridge vlan 1
 no edge-vlan
 l2-tunnel-broadcast-optimization

 qos trust 802.lp
 interface pppoe1
 use firewall-policy default
 cdp holdtime 1000
 cdp timer 900
 service pm sys-restart
 router ospf
nx9500-6C8809(config-profile-default-rfs4000)#
```



## Related Commands

|                              |                              |
|------------------------------|------------------------------|
| <code>no</code> on page 1200 | Disables CDP on this profile |
|------------------------------|------------------------------|

### *cluster*

[Profile Config Commands](#) on page 862

Sets the cluster configuration

#### **Supported in the following platforms:**

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### **Syntax**

```
cluster [force-configured-state|force-configured-state-delay|handle-stp|
master-priority|member|mode|name|radius-counter-db-sync-time]
```

```
cluster [force-configured-state|force-configured-state-delay <3-1800>|
handle-stp| master-priority <1-255>]
```

```
cluster member [ip|vlan]
cluster member [ip <IP> {level [1/2]}|vlan <1-4094>]
```

```
cluster mode [active|standby]
```

```
cluster name <CLUSTER-NAME>
```

```
cluster radius-counter-db-sync-time <1-1440>
```

#### **Parameters**

```
cluster [force-configured-state|force-configured-state-delay <3-1800>|handle-stp|master-
priority <1-255>]
```

|                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>force-configured-state</b>                      | <p>Forces adopted APs to auto revert when a failed wireless controller or service platform (in a cluster) restarts</p> <p>When an active controller (wireless controller, or service platform) fails, a standby controller in the cluster takes over APs adopted by the failed active controller. If the failed active controller were to restart, it starts a timer based on the 'force-configured-state-delay' interval specified. At the expiration of this interval, the standby controller releases all adopted APs and goes back to a monitoring mode. If the active controller fails during this interval, the 'force-configured-state-delay' timer is stopped. The timer restarts as soon as the active controller comes back up.</p> <p>This feature is disabled by default.</p> |
| <b>force-configured-state-delay &lt;3-1800&gt;</b> | <p>Forces cluster transition to the configured state after a specified interval</p> <ul style="list-style-type: none"> <li>• &lt;3-1800&gt; – Specify a delay from 3 - 1800 minutes. The default is 5 minutes.</li> </ul> <p>This is the interval a standby controller waits before releasing adopted APs when a failed primary controller becomes active again.</p>                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>handle-stp</b>                                  | <p>Enables Spanning Tree Protocol (STP) convergence handling. This feature is disabled by default.</p> <p>In layer 2 networks, this protocol is enabled to prevent network looping. If enabled, the network forwards data only after STP convergence. Enabling STP convergence delays the redundancy state machine execution until the STP convergence is completed (the standard protocol value for STP convergence is 50 seconds). Delaying the state machine is important to load balance APs at startup.</p>                                                                                                                                                                                                                                                                          |
| <b>master-priority &lt;1-255&gt;</b>               | <p>Configures cluster master priority</p> <ul style="list-style-type: none"> <li>• &lt;1-255&gt; – Specifies cluster master election priority. Assign a value from 1 - 255. Higher the value higher is the precedence. The default is 128.</li> </ul> <p>In a cluster environment one device from the cluster is elected as the cluster master. A device's master priority value decides the device's priority to become cluster master.</p>                                                                                                                                                                                                                                                                                                                                              |

```
cluster member [ip <IP> {level [1|2]}|vlan <1-4094>]
```

|                                  |                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>member</b>                    | <p>Adds a member to the cluster. It also configures the cluster VLAN where members can be reached.</p>                                                                                                                                                                                                                                                                              |
| <b>ip &lt;IP&gt; level [1 2]</b> | <p>Adds IP address of the new cluster member</p> <ul style="list-style-type: none"> <li>• &lt;IP&gt; – Specify the IP address.</li> <li>• level – Optional. Configures routing level for the new member. Select one of the following routing levels: <ul style="list-style-type: none"> <li>1 - Level 1, local routing</li> <li>2 - Level 2, In-site routing</li> </ul> </li> </ul> |
| <b>vlan &lt;1-4094&gt;</b>       | <p>Configures the cluster VLAN where members can be reached</p> <ul style="list-style-type: none"> <li>• &lt;1-4094&gt; – Specify the VLAN ID from 1- 4094.</li> </ul>                                                                                                                                                                                                              |

```
cluster mode [active|standby]
```

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mode [active standby]</b> | <p>Configures cluster member's mode as active or standby</p> <ul style="list-style-type: none"> <li>• active – Configures cluster mode as active. This is the default setting.</li> <li>• standby – Configures cluster mode as standby</li> </ul> <p>A member can be in either an Active or Standby mode. All active member controllers can adopt access points. Standby members only adopt access points when an active member has failed or sees an access point not adopted by a controller.</p> |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
cluster name <CLUSTER-NAME>
```



|                                  |                                                                                                                                |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>name &lt;CLUSTER-NAME&gt;</b> | Configures the cluster name <ul style="list-style-type: none"><li>• &lt;CLUSTER-NAME&gt; - Specify the cluster name.</li></ul> |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------|

```
cluster radius-counter-db-sync-time <1-1440>
```

|                                                   |                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>radius-counter-db-sync-time &lt;1-1440&gt;</b> | Configures the interval, in minutes, at which the RADIUS counter database is synchronized with the dedicated NTP server resource. <ul style="list-style-type: none"><li>• &lt;1-1440&gt; - Specify a value from 1 - 1440 minutes. The default is 5 minutes.</li></ul> Use the <code>show &gt; cluster &gt; configuration</code> command to view RADIUS counter DB sync time. |
|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Example**

```
nx9500-6C8809(config-profile-default-rfs4000)#cluster name cluster1
nx9500-6C8809(config-profile-default-rfs4000)#cluster member ip 172.16.10.3
nx9500-6C8809(config-profile-default-rfs4000)#cluster mode active

nx9500-6C8809(config-profile-default-rfs4000)#show context
profile rfs4000 default-rfs4000
 bridge vlan 1
 description Vlan1

 cluster name cluster1
 cluster member ip 172.16.10.3
 cluster member vlan 1
nx9500-6C8809(config-profile-default-rfs4000)#
```

**Related Commands**

|                        |                        |
|------------------------|------------------------|
| <b>no</b> on page 1200 | Removes cluster member |
|------------------------|------------------------|

*configuration-persistence*

[Profile Config Commands](#) on page 862

Enables configuration persistence across reloads. This option is enabled by default.

**Supported in the following platforms:**

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
configuration-persistence {auto|secure}
```

**Parameters**

```
configuration-persistence {auto|secure}
```



|               |                                                                                                     |
|---------------|-----------------------------------------------------------------------------------------------------|
| <b>auto</b>   | Optional. Assigns default value based on the device type                                            |
| <b>secure</b> | Optional. Ensures parts of a file that contain security information are not written during a reload |

### Example

```

nx9500-6C8809(config-profile-default-rfs4000)#configuration-persistence secure

nx9500-6C8809(config-profile-default-rfs4000)#show context
profile rfs4000 default-rfs4000
 bridge vlan 1
 no edge-vlan
 ip igmp snooping
 no ip igmp snooping unknown-multicast-fwd
 no ip igmp snooping mrouter learn pim-dvmrp
 autoinstall configuration
 autoinstall firmware

 cluster name cluster1
 cluster member ip 1.2.3.4 level 2
 cluster member ip 172.16.10.3
 cluster member vlan 4094
 cluster handle-stp
 cluster force-configured-state
 holdtime 1000
 timer 900
 configuration-persistence secure
nx9500-6C8809(config-profile-default-rfs4000)#

```

### Related Commands

|                        |                                                           |
|------------------------|-----------------------------------------------------------|
| <b>no</b> on page 1200 | Disables automatic write up of startup configuration file |
|------------------------|-----------------------------------------------------------|

## controller

[Profile Config Commands](#) on page 862

Configures the WiNG controller (wireless controller or service platform) adoption settings

Adoption is the process a controller or service platform uses to discover available access points and/or peer controllers/service platforms, establish an association and provision the adopted device. Adoption settings are configurable and supported within a profile and applied to all devices supported by the profile.

Use this command to add a controller to a pool and group. This command also enables and disables adoption on controllers, and specifies the device types that can be adopted by a controller.

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

## Syntax

```
controller [adopted-devices|adoption|group|hello-interval|vlan|host]
```

```
controller adopted-devices [aps {controllers}|controllers {aps}/external-devices|external-devices-monitoring-only]hel
```

```
controller adoption
```

```
controller [group <CONTROLLER-GROUP-NAME>|vlan <1-4094>]
```

```
controller hello-interval <1-120> adjacency-hold-time <2-600>
```

```
controller host [<IPv4>|<IPv6>|<HOSTNAME>] {ipsec-secure|level|pool|remote-vpn-client}
```

```
controller host [<IPv4>|<IPv6>|<HOSTNAME>] {ipsec-secure} {gw [<IP>|<HOSTNAME>]}
```

```
controller host [<IPv4>|<IPv6>|<HOSTNAME>] {level [1/2]|pool <1-2> level [1/2]} {ipsec-secure {gw [<IP>|<HOSTNAME>]}}|remote-vpn-client}
```

```
controller host [<IPv4>|<IPv6>|<HOSTNAME>] {remote-vpn-client}
```

## Parameters

```
controller adopted-devices [aps {controllers}|controllers {aps}|external-devices|external-devices-monitoring-only]
```

|                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>controller</b>                         | Configures the WLAN's controller adoption settings                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>adopted-devices</b>                    | Configures the types of device (AP/controller) this controller can adopt                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>aps</b><br><b>{<i>controllers</i>}</b> | Enables the adoption of network access points by this controller. This option is enabled by default. <ul style="list-style-type: none"><li>• <i>controllers</i> - Optional. Enables the adoption of peer controllers by this controller</li></ul> All adopted devices (referred to as adoptee) receive complete configuration from the adopting controller (referred to as adopter).                                                                                                    |
| <b>controllers</b><br><b>{<i>aps</i>}</b> | Enables the adoption of peer controllers by this controllers <ul style="list-style-type: none"><li>• <i>aps</i> - Optional. Enables the adoption of network access points by this controller</li></ul> A controller cannot be configured as an adoptee and an adopter simultaneously. In other words, an adopted controller (adoptee) cannot be configured to adopt another controller.<br>Use the <code>no &gt; controller &gt; adopted-devices</code> command to remove this setting. |

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>external-devices</b>                 | <p>Enables adoption of external devices by this controller. This option is disabled by default.</p> <p>When enabled, a WiNG controller can adopt and manage T5 controllers and EX3500 switches (using the IPX operating system) within a WiNG managed device subnet. This setting is disabled by default.</p> <p>To disable T5 or EX3500 adoption, use the <code>no &gt; controller &gt; external-devices</code> command.</p> <p>This feature is supported only on RFS4000, NX9500, NX9510, NX9600, and VX9000 platforms.</p> |
| <b>external-devices-monitoring-only</b> | <p>Enables only monitoring of external devices by this controller or service platform. This option is disabled by default.</p>                                                                                                                                                                                                                                                                                                                                                                                                |

controller adoption

|                            |                                                                                                                                                                                                                                                |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>controller adoption</b> | <p>Enables the adoption of the logged device (wireless controller or service platform) by other controllers. This option is disabled by default.</p> <p>Use the <code>no &gt; controller &gt; adoption</code> command to disable adoption.</p> |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

controller [group <CONTROLLER-GROUP-NAME>|vlan <1-4094>]

|                                            |                                                                                                                                                                                                                         |
|--------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>controller</b>                          | Configures the WLAN's controller adoption settings                                                                                                                                                                      |
| <b>group &lt;CONTROLLER-GROUP-NAME&gt;</b> | <p>Configures the wireless controller or service platform group</p> <ul style="list-style-type: none"> <li>• &lt;CONTROLLER-GROUP-NAME&gt; - Specify the wireless controller or service platform group name.</li> </ul> |
| <b>vlan &lt;1-4094&gt;</b>                 | <p>Configures the wireless controller or service platform VLAN</p> <ul style="list-style-type: none"> <li>• &lt;1-4094&gt; - Specify the VLAN ID from 1 - 4094.</li> </ul>                                              |

controller hello-interval <1-120> adjacency-hold-time <2-600>

|                                          |                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>controller</b>                        | Configures the WLAN's controller settings                                                                                                                                                                                                                                                                                                        |
| <b>hello-interval &lt;1-120&gt;</b>      | <p>Configures the hello-interval in seconds. This is the interval between consecutive hello packets exchanged between AP and wireless controller or service platform.</p> <ul style="list-style-type: none"> <li>• &lt;1-120&gt; - Specify a value from 1 - 120 seconds.</li> </ul>                                                              |
| <b>adjacency-hold-time &lt;2-600&gt;</b> | <p>Configures the adjacency hold time in seconds. This is the time since the last received hello packet, after which the adjacency between wireless controller or service platform and AP is lost, and the link is re-established.</p> <ul style="list-style-type: none"> <li>• &lt;2-600&gt; - Specify a value from 2 - 600 seconds.</li> </ul> |

controller host [<IPv4>|<IPv6>|<HOSTNAME>] {ipsec-secure} {gw [<IP>|<HOSTNAME>]}

|                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>controller</b>                                                                   | Configures the WLAN's controller adoption settings                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>host</b> [ <b>&lt;IPv4&gt;</b>   <b>&lt;IPv6&gt;</b>   <b>&lt;HOSTNAME&gt;</b> ] | Configures wireless controller or service platform's IPv4/IPv6 address or hostname <ul style="list-style-type: none"> <li>• &lt;IPv4&gt; – Configures wireless controller or service platform's IPv4 address</li> <li>• &lt;IPv6&gt; – Configures wireless controller or service platform's IPv6 address</li> <li>• &lt;HOSTNAME&gt; – Configures wireless controller or service platform's hostname</li> </ul>                                                                                                                                                                                                                                                             |
| <b>ipsec-secure</b> { <b>gw</b> [ <b>&lt;IP&gt;</b>   <b>&lt;HOSTNAME&gt;</b> ] }   | Optional. Enables Internet Protocol Security (IPSec) peer authentication on the connection (link) between the adopting devices. This option is disabled by default. <ul style="list-style-type: none"> <li>• gw – Optional. Specifies a IPSec gateway other than the wireless controller or service platform <ul style="list-style-type: none"> <li>• &lt;IP&gt; – Use this option to specify the IPSec gateway's IP address.</li> <li>• &lt;HOSTNAME&gt; – Use this option to specify the IPSec gateway's hostname.</li> </ul> </li> </ul> <p>If the gateway's IP address or hostname is not specified, the system assumes the logged controller as the IPSec gateway.</p> |

```
controller host [<IPv4>|<IPv6>|<HOSTNAME>] {level [1|2]|pool <1-2> level [1|2]} {ipsec-secure {gw [<IP>|<HOSTNAME>]}|remote-vpn-client}
```

|                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>controller</b>                                                                   | Configures the WLAN's controller adoption settings                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>host</b> [ <b>&lt;IPv4&gt;</b>   <b>&lt;IPv6&gt;</b>   <b>&lt;HOSTNAME&gt;</b> ] | Configures wireless controller or service platform's IPv4/IPv6 address or name <ul style="list-style-type: none"> <li>• &lt;IPv4&gt; – Configures wireless controller or service platform's IPv4 address</li> <li>• &lt;IPv6&gt; – Configures wireless controller or service platform's IPv6 address</li> <li>• &lt;HOSTNAME&gt; – Configures wireless controller or service platform's name</li> </ul>                                                                                                       |
| <b>level</b> [ <b>1</b>   <b>2</b> ]                                                | The following keywords are common to the 'IP', 'IPv6', and 'hostname' parameters: Optional. After providing the wireless controller or service platform's address, optionally select one of the following routing levels: <ul style="list-style-type: none"> <li>• 1 – Optional. Level 1, local routing</li> <li>• 2 – Optional. Level 2, inter-site routing</li> </ul> <p><b>Note:</b> After specifying the routing level, you can, optionally enable IPSec Secure authentication and remote VPN client.</p> |
| <b>pool</b> <b>&lt;1-2&gt;</b> <b>level</b> [ <b>1</b>   <b>2</b> ]                 | The following keywords are common to the 'IP', 'IPv6', and 'hostname' parameters: Optional. Sets the wireless controller or service platform's pool <ul style="list-style-type: none"> <li>• &lt;1-2&gt; – Select either 1 or 2 as the pool. The default is 1. After selecting the pool, optionally select one of the following two routing levels: <ul style="list-style-type: none"> <li>• 1 – Optional. Level 1, local routing</li> <li>• 2 – Optional. Level 2, inter-site routing</li> </ul> </li> </ul> |

|                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>{ipsec-secure  {gw [&lt;IP&gt;   &lt;HOSTNAME&gt;]}   remote-vpn-  client}</pre> | <p>After specifying the routing level and or device's pool, you can optionally specify the following:</p> <ul style="list-style-type: none"> <li>ipsec-secure - Optional. Enables IPSec peer authentication on the connection (link) between the adopting devices. This option is disabled by default.</li> <li>gw - Optional. Specifies a IPSec gateway other than the wireless controller or service platform <ul style="list-style-type: none"> <li>&lt;IP&gt; - Use this option to specify the IPSec gateway's IP address.</li> <li>&lt;HOSTNAME&gt; - Use this option to specify the IPSec gateway's hostname.</li> </ul> </li> </ul> <p><b>Note:</b> If the gateway's IP address or hostname is not specified, the system assumes the logged controller as the IPSec gateway.</p> |
|                                                                                       | <ul style="list-style-type: none"> <li>remote-vpn-client - Forces MiNT link creation protocol (MLCP) to use remote VPN connection on the controller</li> </ul> <p>The controller uses remote VPN tunnel for this traffic. If multiple controller hosts are configured, either all the hosts should use remote-vpn-client or none. When enabled, an MLCP connection is not initiated until remote VPN connection is UP and virtual IP, DNS server, source route, etc. are installed on the AP.</p>                                                                                                                                                                                                                                                                                       |

```
controller host [<IPv4>|<IPv6>|<HOSTNAME>] {remote-vpn-client}
```

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>controller</b>                      | Configures the WLAN's controller settings                                                                                                                                                                                                                                                                                                                                                                  |
| <b>host</b> [<IPv4> <IPv6> <HOSTNAME>] | <p>Configures wireless controller or service platform's IPv4/IPv6 address or hostname</p> <ul style="list-style-type: none"> <li>&lt;IP&gt; - Configures wireless controller or service platform's IPv4 address</li> <li>&lt;IPv6&gt; - Configures wireless controller or service platform's IPv6 address</li> <li>&lt;HOSTNAME&gt; - Configures wireless controller or service platform's name</li> </ul> |
| <b>remote-vpn-client</b>               | <p>Forces MLCP to use remote VPN connection on the controller</p> <p>The controller uses remote VPN tunnel for this traffic. If multiple controller hosts are configured, either all the hosts should use remote-vpn-client or none. When enabled, an MLCP connection is not initiated until remote VPN connection is UP and virtual IP, DNS server, source route, etc. are installed on the AP.</p>       |

### Example

```
rfs6000-37FABEnx9500-6C8809(config-profile-default-rfs4000)controller group test
nx9500-6C8809(config-profile-default-rfs4000)#controller host 1.2.3.4 pool 2

rfs7000-37FABE(config-profile-default-rfs4000)#show context
profile rfs4000 default-rfs4000
no autoinstall configuration
no autoinstall firmware
crypto isakmp policy default
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
.....
interface ge4
ip dhcp trust
qos trust dscp
qos trust 802.1p
use firewall-policy default
controller host 1.2.3.4 pool 2
controller group test
service pm sys-restart
--More--
nx9500-6C8809(config-profile-default-rfs4000)#
```

```

rfs4000-229D58(config-profile-testRFS4000)#controller adopted-devices aps controllers

rfs4000-229D58(config-profile-testRFS4000)#show context
profile rfs4000 testRFS4000
 autoinstall configuration

 logging on
 service pm sys-restart
 router ospf
 controller adopted-devices aps controllers
rfs4000-229D58(config-profile-testRFS4000)#

```

### Related Commands

|                 |                                               |
|-----------------|-----------------------------------------------|
| no on page 1200 | Disables or reverts settings to their default |
|-----------------|-----------------------------------------------|

### *critical-resource*

[Profile Config Commands](#) on page 862

Enables monitoring of resources critical to the health of the service platform, wireless controller, or access point managed network. These critical resources are identified by their configured IP addresses. When enabled, the system monitors these devices regularly and logs their status. Use this command to create a critical resource monitoring (CRM) policy.

A critical resource can be a gateway, AAA server, WAN interface, any hardware, or a service on which the stability of the network depends. Monitoring these resources is therefore essential. When enabled, this feature pings critical resources regularly to ascertain their status. If there is a connectivity issue, an event is generated stating a critical resource is unavailable. By default, there is no enabled critical resource policy and one needs to be created and implemented.

Critical resources can be monitored directly through the interfaces on which they are discovered. For example, a critical resource on the same subnet as an AP8132 access point can be monitored by its IP address. However, a critical resource located on a VLAN must continue to be monitored on that VLAN.

Critical resource monitoring can be enabled on service platforms, wireless controllers, and access points through their respective device profiles.

#### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
critical-resource [<CR-NAME>|monitor|retry-count]
```

```
critical-resource <CR-NAME> [monitor|monitor-using-flows]
```

```
critical-resource <CR-NAME> monitor [direct|via]
```

```
critical-resource <CR-NAME> monitor direct [all|any] [<IP/HOST-ALIAS-NAME>|sync-adoptees] {<IP/HOST-ALIAS-NAME>/arp-only vlan [<1-4094>|<VLAN-ALIAS-NAME>]}<IP/HOST-ALIAS-NAME>/port [<LAYER2-IF-NAME>/ge <1-4>|port-channel <1-2>]}
```

```
critical-resource <CR-NAME> monitor via [<IP/HOST-ALIAS-NAME>|<LAYER3-INTERFACE-NAME>|pppoe1|vlan|wwan1]
```

```
critical-resource <CR-NAME> monitor via [<IP/HOST-ALIAS-NAME>|<LAYER3-INTERFACE-NAME>|pppoe1|vlan <1-4094>|wwan1] [all|any] [<IP/HOST-ALIAS-NAME>| sync-adoptees] {<IP/HOST-ALIAS-NAME>/arp-only [vlan <1-4094>|<VLAN-ALIAS-NAME>]}<IP/HOST-ALIAS-NAME>/port [<LAYER2-IF-NAME>/ge <1-4>|port-channel <1-2>]}
```

```
critical-resource <CR-NAME> monitor-using-flows [all|any] [criteria|dhcp|dns|sync-adoptees]
```

```
critical-resource <CR-NAME> monitor-using-flows [all|any] criteria [all|cluster-master|rf-domain-manager] (dhcp [vlan <1-4094>|<VLAN-ALIAS-NAME>]| dns <IP/HOST-ALIAS-NAME>)} {dhcp vlan [<1-4094>|<VLAN-ALIAS-NAME>]|/dns <IP/HOST-ALIAS-NAME>}
```

```
critical-resource <CR-NAME> monitor-using-flows [all|any] dhcp vlan <1-4094> {dhcp vlan [<1-4094>|<VLAN-ALIAS-NAME>]|/dns <IP/HOST-ALIAS-NAME>}
```

```
critical-resource <CR-NAME> monitor-using-flows [all|any] dns <IP/HOST-ALIAS-NAME> {dhcp [vlan <1-4094>|<VLAN-ALIAS-NAME>]|/dns <IP/HOST-ALIAS-NAME>}
```

```
critical-resource <CR-NAME> monitor-using-flows [all|any] sync-adoptees criteria [all|cluster-master|rf-domain-manager] (dhcp [vlan <1-4094>|<VLAN-ALIAS-NAME>]|/dns <IP/HOST-ALIAS-NAME>)} {dhcp [vlan <1-4094>|<VLAN-ALIAS-NAME>]|/dns <IP/HOST-ALIAS-NAME>}
```

```
critical-resource monitor interval <5-86400>
```

```
critical-resource retry-count <0-10>
```

### Parameters

```
critical-resource <CR-NAME> monitor direct [all|any] [<IP/HOST-ALIAS-NAME>|sync-adoptees] {<IP/HOST-ALIAS-NAME>|arp-only [vlan <1-4094>|<VLAN-ALIAS-NAME>]}<IP/HOST-ALIAS-NAME>|port [<LAYER2-IF-NAME>/ge <1-4>|port-channel <1-2>]}
```

|                        |                                                                                              |
|------------------------|----------------------------------------------------------------------------------------------|
| <b>&lt;CR-NAME&gt;</b> | Identifies the critical resource to be monitored. Provide the name of the critical resource. |
| <b>monitor</b>         | Enables critical resource(s) monitoring                                                      |



|                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>direct</b> [ <b>all</b>   <b>any</b> ]<br>[<IP/HOST-ALIAS-NAME>  <b>sync-adoptees</b> ]                                                            | Monitors critical resources using the default routing engine <ul style="list-style-type: none"> <li>all - Monitors all resources that are going down (generates an event when all specified critical resources are unreachable)</li> <li>any - Monitors any resource that is going down (generates an event when any one of the specified critical resource is unreachable) <ul style="list-style-type: none"> <li>&lt;IP/HOST-ALIAS-NAME&gt; - Configures the IP address of the critical resource being monitored (for example, the DHCP or DNS server). Specify the IP address in the A.B.C.D format. You can use a host-alias to identify the critical resource. If using a host-alias, ensure that the host-alias is existing and configured.</li> </ul> </li> <li>sync-adoptees - Syncs adopted access points with the controller. In the stand-alone AP scenario, where the CRM policy is running on the AP, the AP is directly intimated in case a critical resource goes down. On the other hand, when an AP is adopted to a controller (running the CRM policy), it is essential to enable the sync-adoptees option in order to sync the AP with the controller regarding the latest CRM status.</li> </ul> |
| <b>arp-only vlan</b><br>[<1-4094> <VLAN-ALIAS-NAME>]<br>{<IP/HOST-ALIAS-NAME>  <b>port</b><br>[<LAYER2-IFNAME>  <b>ge</b>  <br><b>port-channel</b> ]} | The following keywords are common to the 'all' and 'any' parameters: <ul style="list-style-type: none"> <li>arp-only vlan &lt;1-4094&gt; - Optional. Uses ARP to determine if the IP address is reachable (use this option to monitor resources that do not have IP addresses). ARP is used to resolve hardware addresses when only the network layer address is known.</li> <li>vlan [&lt;1-4094&gt; &lt;VLAN-ALIAS-NAME&gt;] - Specifies the VLAN ID on which to send the probing ARP requests. Specify the VLAN ID from 1 - 4094. Alternately, use a vlan-alias to identify the VLAN. If using a vlan-alias, ensure that the alias is existing and configured. <ul style="list-style-type: none"> <li>&lt;IP/HOST-ALIAS-NAME&gt; - Optional. Limits ARP to a device specified by the &lt;IP&gt; parameter. You can use a host-alias to specify the IP address. If using a host-alias, ensure that the host-alias is existing and configured.</li> <li>port [&lt;LAYER2-IF-NAME&gt; <b>ge</b> <b>port-channel</b>] - Optional. Limits ARP to a specified port</li> </ul> </li> </ul>                                                                                                                               |

```
critical-resource <CRM-POLICY-NAME> monitor via [<IP/HOST-ALIAS-NAME>|<LAYER3-INTERFACE-NAME>|pppoe1|vlan <1-4094>|wwan1] [all|any] [<IP/HOST-ALIAS-NAME>| sync-adoptees] {<IP/HOST-ALIAS-NAME>|arp-only vlan [<1-4094>|<VLAN-ALIAS-NAME>] {<IP>|port [<LAYER2-IFNAME>|ge|port-channel]}}
```

|                                      |                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;CR-NAME&gt;</b>               | Identifies the critical resource to be monitored. Provide the name of the critical resource.                                                                                                                                                                                                                                                                          |
| <b>monitor</b>                       | Enables critical resource(s) monitoring                                                                                                                                                                                                                                                                                                                               |
| <b>via</b>                           | Specifies the interface or next-hop via which the ICMP pings should be sent. Configures the interface or next-hop via which ICMP pings are sent. This does not apply to IP addresses configured for arp-only. For interfaces which learn the default-gateway dynamically (like DHCP clients and PPP interfaces), use an interface name for VIA, or use an IP address. |
| <b>&lt;IP/HOST-ALIAS-NAME&gt;</b>    | Specify the IP address of the next-hop via which the critical resource(s) are monitored. Configures up to four IP addresses for monitoring. All the four IP addresses constitute critical resources. You can use a host-alias to specify the IP address. If using a host-alias, ensure that the host-alias is existing and configured.                                |
| <b>&lt;LAYER3-INTERFACE-NAME&gt;</b> | Specify the layer 3 Interface name (router interface)                                                                                                                                                                                                                                                                                                                 |
| <b>pppoe1</b>                        | Specifies PPP over Ethernet interface                                                                                                                                                                                                                                                                                                                                 |

|                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vlan</b> [ <b>&lt;1-4094&gt;</b>   <b>&lt;VLAN-ALIAS-NAME&gt;</b> ]                                                                                                                                 | Specifies the wireless controller or service platform's VLAN interface. Specify VLAN ID from 1 - 4094. Alternately, use a vlan-alias to identify the VLAN. If using a vlan-alias, ensure that the alias is existing and configured.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>wwan1</b>                                                                                                                                                                                           | Specifies Wireless WAN interface                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>[all any]</b> [ <b>&lt;IP/HOST-ALIAS-NAME&gt;</b>   <b>sync-adoptees</b> ]                                                                                                                          | Monitors critical resources using the default routing engine <ul style="list-style-type: none"> <li>all - Monitors all resources that are going down (generates an event when all specified critical resource IP addresses are unreachable)</li> <li>any - Monitors any resource that is going down (generates an event when any one of the specified critical resource IP address is unreachable) <ul style="list-style-type: none"> <li>&lt;IP/HOST-ALIAS-NAME&gt; - Configures the IP address of the critical resource being monitored (for example, the DHCP or DNS server). Specify the IP address in the A.B.C.D format. You can use a host-alias to specify the IP address. If using a host-alias, ensure that the host-alias is existing and configured.</li> </ul> </li> <li>sync-adoptees - Syncs adopted access points with the controller. In the stand-alone AP scenario, where the CRM policy is running on the AP, the AP is directly intimated in case a critical resource goes down. On the other hand, when an AP is adopted to a controller (running the CRM policy), it is essential to enable the sync-adoptees option in order to sync the AP with the controller regarding the latest CRM status.</li> </ul> |
| <b>arp-only vlan</b> [ <b>&lt;1-4094&gt;</b>   <b>&lt;VLAN-ALIAS-NAME&gt;</b> ] { <b>&lt;IP/HOST-ALIAS-NAME&gt;</b>   <b>port</b> [ <b>&lt;LAYER2-IFNAME&gt;</b>   <b>ge</b>   <b>port-channel</b> ] } | The following keywords are common to the 'all' and 'any' parameters: <ul style="list-style-type: none"> <li>arp-only vlan &lt;1-4094&gt; - Optional. Uses ARP to determine if the IP address is reachable (use this option to monitor resources that do not have IP addresses). ARP is used to resolve hardware addresses when only the network layer address is known.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                                                                                                                                                                                                        | <ul style="list-style-type: none"> <li>vlan [<b>&lt;1-4094&gt;</b> <b>&lt;VLAN-ALIAS-NAME&gt;</b>] - Specifies the VLAN ID to send the probing ARP requests. Specify the VLAN ID from 1 - 4094. Alternately, use a vlan-alias to identify the VLAN. If using a vlan-alias, ensure that the alias is existing and configured.</li> <li>&lt;IP'HOST-ALIAS-NAME&gt; - Optional. Limits ARP to a device specified by the &lt;IP&gt; parameter. You can use a host-alias to specify the IP address. If using a host-alias, ensure that the host-alias is existing and configured.</li> <li>port [<b>&lt;LAYER2-IF-NAME&gt;</b> <b>ge</b> <b>port-channel</b>] - Optional. Limits ARP to a specified port</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

```
critical-resource <CRM-POLICY-NAME> monitor-using-flows [all|any] criteria [all|cluster-master|rf-domain-manager] (dhcp [vlan <1-4094>|<VLAN-ALIAS-NAME>]| dns <IP/HOST-ALIAS-NAME>) {dhcp [vlan <1-4094>|<VLAN-ALIAS-NAME>]|dns <IP/HOST-ALIAS-NAME>}
```

|                            |                                                                                                                                                                                                       |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;CR-NAME&gt;</b>     | Identifies the critical resource to be monitored. Provide the name of the critical resource.                                                                                                          |
| <b>monitor-using-flows</b> | Enables critical resource(s) monitoring using message flows for DHCP or DNS (DHCP discover, DHCP offer, etc.) instead of ICMP or ARP packets in order to reduce the amount of traffic on the network. |

|                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[all any]</b>                                                                              | <p>Configures how critical resource event messages are generated. Options include all and any.</p> <ul style="list-style-type: none"> <li>all – Monitors all resources that are going down (generates an event when all specified critical resources are unreachable)</li> <li>any – Monitors any resource that is going down (generates an event when any one of the specified critical resource is unreachable)</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>criteria [all cluster-master rf-domain-manager]</b>                                        | <p>Configures the resource that will monitor critical resources and update the rest of the devices in a group. Options include all, rf-domain-manager, or cluster-master.</p> <ul style="list-style-type: none"> <li>all – Configures all devices within a group (cluster or RF Domain) as the monitoring resource</li> <li>cluster-master – Configures the cluster master as the monitoring resource</li> <li>rf-domain-manager – Configures the RF Domain manager as the monitoring resource</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>dhcp vlan [&lt;1-4094&gt; &lt;VLAN-ALIAS-NAME&gt;]</b>                                     | <p>The following parameters are recursive and common to the 'all', 'cluster-master', and 'rf-domain-manager' keywords:</p> <ul style="list-style-type: none"> <li>dhcp – Configures DHCP as the mode of monitoring critical resources. When configured, DHCP message flows (DHCP Discover, DHCP Offer, etc.) are used instead of ICMP or ARP packets to confirm critical resource availability. <ul style="list-style-type: none"> <li>vlan [&lt;1-4094&gt; &lt;VLAN-ALIAS-NAME&gt;] – Configures the VLAN on which the critical resource(s) is available. Specify the VLAN from 1 - 4094. Alternately, use a vlan-alias to identify the VLAN. If using a vlan-alias, ensure that the alias is existing and configured.</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>dns &lt;IP/HOST-ALIAS-NAME&gt;</b>                                                         | <p>The following parameters are recursive and common to the 'all', 'cluster-master', and 'rf-domain-manager' keywords:</p> <ul style="list-style-type: none"> <li>dns – Configures DNS as the mode of monitoring critical resources. When configured, DNS message flows are used instead of ICMP or ARP packets to confirm critical resource availability. <ul style="list-style-type: none"> <li>&lt;IP/HOST-ALIAS-NAME&gt; – Configures the IPv4 address or host alias of the critical resource. Specify the IPv4 address or host alias name (should be existing and configured).</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>{dhcp [vlan [&lt;1-4094&gt; &lt;VLAN-ALIAS-NAME&gt;]  dns &lt;IP/HOST-ALIAS-NAME&gt;]}</b> | <p>The 'dhcp' and 'dns' parameters are recursive and you can optionally configure multiple VLANs and critical resource IPv4 addresses (or host alias names).</p> <ul style="list-style-type: none"> <li>dhcp – Optional. Configures DHCP as the mode of monitoring critical resources. When configured, DHCP message flows (DHCP Discover, DHCP Offer, etc.) are used instead of ICMP or ARP packets to confirm critical resource availability. <ul style="list-style-type: none"> <li>vlan [&lt;1-4094&gt; &lt;VLAN-ALIAS-NAME&gt;] – Configures the VLAN on which the critical resource(s) is available. Specify the VLAN from 1 - 4094. Alternately, use a vlan-alias to identify the VLAN. If using a vlan-alias, ensure that the alias is existing and configured.</li> </ul> </li> <li>dns – Optional. Configures DNS as the mode of monitoring critical resources. When configured, DNS message flows are used instead of ICMP or ARP packets to confirm critical resource availability. <ul style="list-style-type: none"> <li>&lt;IP/HOST-ALIAS-NAME&gt; – Configures the IPv4 address or host alias of the critical resource. Specify the IPv4 address or host alias name (should be existing and configured).</li> </ul> </li> </ul> |

```
critical-resource <CRM-POLICY-NAME> monitor-using-flows [all|any] dhcp vlan [<1-4094>|<VLAN-ALIAS-NAME>] {dhcp vlan [<1-4094>|<VLAN-ALIAS-NAME>]|dns <IP/HOST-ALIAS-NAME>}
```

|                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;CR-NAME&gt;</b>                                                                                                                                | Identifies the critical resource to be monitored. Provide the name of the critical resource.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>monitor-using-flows</b>                                                                                                                            | Enables critical resource(s) monitoring using message flows for DHCP or DNS (DHCP Discover, DHCP Offer, etc.) instead of ICMP or ARP packets in order to reduce the amount of traffic on the network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>[all any]</b>                                                                                                                                      | Configures how critical resource event messages are generated. Options include all and any. <ul style="list-style-type: none"> <li>all – Monitors all resources that are going down (generates an event when all specified critical resources are unreachable)</li> <li>any – Monitors any resource that is going down (generates an event when any one of the specified critical resource is unreachable)</li> </ul>                                                                                                                                                                                                                                                                                                                                                               |
| <b>dhcp vlan</b><br><b>[&lt;1-4094&gt;  </b><br><b>&lt;VLAN-ALIAS-</b><br><b>NAME&gt; ]</b>                                                           | Configures DHCP as the mode of monitoring critical resources. When configured, DHCP message flows (DHCP Discover, DHCP Offer, etc.) are used instead of ICMP or ARP packets to confirm critical resource availability. <ul style="list-style-type: none"> <li>vlan [&lt;1-4094&gt; &lt;VLAN-ALIAS-NAME&gt;] – Configures the VLAN on which the critical resource(s) is available. Specify the VLAN from 1 - 4094. Alternately, use a vlan-alias to identify the VLAN. If using a vlan-alias, ensure that the alias is existing and configured.</li> </ul>                                                                                                                                                                                                                           |
| <b>{dhcp vlan</b><br><b>[&lt;1-4094&gt;  </b><br><b>&lt;VLAN-ALIAS-</b><br><b>NAME&gt; ]   dns &lt;IP/</b><br><b>HOST-ALIAS-</b><br><b>NAME&gt; }</b> | The following parameters are recursive and optional. Use them to configure multiple VLANs and critical resource IPv4 addresses (or host alias names): <ul style="list-style-type: none"> <li>dhcp – Optional. Configures DHCP as the mode of monitoring critical resources. When configured, DHCP message flows (DHCP Discover, DHCP Offer, etc.) are used instead of ICMP or ARP packets to confirm critical resource availability. <ul style="list-style-type: none"> <li>vlan [&lt;1-4094&gt; &lt;VLAN-ALIAS-NAME&gt;] – Configures the VLAN on which the critical resource(s) is available. Specify the VLAN from 1 - 4094. Alternately, use a vlan-alias to identify the VLAN. If using a vlan-alias, ensure that the alias is existing and configured.</li> </ul> </li> </ul> |
|                                                                                                                                                       | <ul style="list-style-type: none"> <li>dns – Optional. Configures DNS as the mode of monitoring critical resources. When configured, DNS message flows are used instead of ICMP or ARP packets to confirm critical resource availability. <ul style="list-style-type: none"> <li>&lt;IP/HOST-ALIAS-NAME&gt; – Configures the IPv4 address or host alias of the critical resource. Specify the IPv4 address or host alias name (should be existing and configured).</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                           |

```
critical-resource <CRM-POLICY-NAME> monitor-using-flows [all|any] dns <IP/HOST-ALIAS-NAME>
{dhcp vlan [<1-4094><VLAN-ALIAS-NAME>] | dns <IP/HOST-ALIAS-NAME> }
```

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;CR-NAME&gt;</b>     | Identifies the critical resource to be monitored. Provide the name of the critical resource.                                                                                                                                                                                                                                                                                                                          |
| <b>monitor-using-flows</b> | Enables critical resource(s) monitoring using message flows for DHCP or DNS (DHCP Discover, DHCP Offer, etc.) instead of ICMP or ARP packets in order to reduce the amount of traffic on the network.                                                                                                                                                                                                                 |
| <b>[all any]</b>           | Configures how critical resource event messages are generated. Options include all and any. <ul style="list-style-type: none"> <li>all – Monitors all resources that are going down (generates an event when all specified critical resources are unreachable)</li> <li>any – Monitors any resource that is going down (generates an event when any one of the specified critical resource is unreachable)</li> </ul> |

|                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>dns &lt;IP/HOST-ALIAS-NAME&gt;</b>                                                           | <p>Configures DNS as the mode of monitoring critical resources. When configured, DNS message flows are used instead of ICMP or ARP packets to confirm critical resource availability.</p> <ul style="list-style-type: none"> <li>• &lt;IP/HOST-ALIAS-NAME&gt; - Configures the IPv4 address or host alias of the critical resource. Specify the IPv4 address or host alias name (should be existing and configured).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>{dhcp vlan [ &lt;1-4094&gt;   &lt;VLAN-ALIAS-NAME&gt;   dns &lt;IP/HOST-ALIAS-NAME&gt; }</b> | <p>The following parameters are recursive and optional. Use them to configure multiple VLANs and critical resource IPv4 addresses (or host alias names):</p> <ul style="list-style-type: none"> <li>• dhcp - Optional. Configures DHCP as the mode of monitoring critical resources. When configured, DHCP message flows (DHCP Discover, DHCP Offer, etc.) are used instead of ICMP or ARP packets to confirm critical resource availability. <ul style="list-style-type: none"> <li>• vlan [ &lt;1-4094&gt;   &lt;VLAN-ALIAS-NAME&gt; ] - Configures the VLAN on which the critical resource(s) is available. Specify the VLAN from 1 - 4094. Alternately, use a vlan-alias to identify the VLAN. If using a vlan-alias, ensure that the alias is existing and configured.</li> </ul> </li> <li>• dns - Optional. Configures DNS as the mode of monitoring critical resources. When configured, DNS message flows are used instead of ICMP or ARP packets to confirm critical resource availability. <ul style="list-style-type: none"> <li>• &lt;IP/HOST-ALIAS-NAME&gt; - Configures the IPv4 address or host alias of the critical resource. Specify the IPv4 address or host alias name (should be existing and configured).</li> </ul> </li> </ul> |

```
critical-resource <CRM-POLICY-NAME> monitor-using-flows [all|any] sync-adoptees criteria [all|cluster-master|rf-domain-manager] (dhcp vlan [<1-4094> | <VLAN-ALIAS-NAME>] | dns <IP/HOST-ALIAS-NAME>) {dhcp vlan [<1-4094> | <VLAN-ALIAS-NAME>] | dns <IP/HOST-ALIAS-NAME> }
```

|                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;CR-NAME&gt;</b>                                 | Identifies the critical resource to be monitored. Provide the name of the critical resource.                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>monitor-using-flows</b>                             | Enables critical resource(s) monitoring using message flows for DHCP or DNS (DHCP Discover, DHCP Offer, etc.) instead of ICMP or ARP packets in order to reduce the amount of traffic on the network.                                                                                                                                                                                                                                                                                                           |
| <b>[all any]</b>                                       | <p>Configures how critical resource event messages are generated. Options include all and any.</p> <ul style="list-style-type: none"> <li>• all - Monitors all resources that are going down (generates an event when all specified critical resources are unreachable)</li> <li>• any - Monitors any resource that is going down (generates an event when any one of the specified critical resource is unreachable)</li> </ul>                                                                                |
| <b>syn-adoptees</b>                                    | Syncs adopted access points with the controller. In the stand-alone AP scenario, where the CRM policy is running on the AP, the AP is directly intimated in case a critical resource goes down. On the other hand, when an AP is adopted to a controller (running the CRM policy), it is essential to enable the sync-adoptees option in order to sync the AP with the controller regarding the latest CRM status.                                                                                              |
| <b>criteria [all cluster-master rf-domain-manager]</b> | <p>Configures the resource that will monitor critical resources and update the rest of the devices in a group. Options include all, rf-domain-manager, or cluster-master.</p> <ul style="list-style-type: none"> <li>• all - Configures all devices within a group (cluster or RF Domain) as the monitoring resource</li> <li>• cluster-master - Configures the cluster master as the monitoring resource</li> <li>• rf-domain-manager - Configures the RF Domain manager as the monitoring resource</li> </ul> |

|                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>dhcp vlan</b><br><b>[&lt;1-4094&gt;  </b><br><b>&lt;VLAN-ALIAS-</b><br><b>NAME&gt;]</b>                                                          | <p>The following parameters are recursive and common to the 'all', 'cluster-master', and 'rf-domain-manager' keywords:</p> <ul style="list-style-type: none"> <li>• <b>dhcp</b> - Configures DHCP as the mode of monitoring critical resources. When configured, DHCP message flows (DHCP Discover, DHCP Offer, etc.) are used instead of ICMP or ARP packets to confirm critical resource availability.</li> <li>• <b>vlan [&lt;1-4094&gt; &lt;VLAN-ALIAS-NAME&gt;]</b> - Configures the VLAN on which the critical resource(s) is available. Specify the VLAN from 1 - 4094. Alternately, use a vlan-alias to identify the VLAN. If using a vlan-alias, ensure that the alias is existing and configured.</li> </ul>                                                 |
| <b>dns &lt;IP/HOST-</b><br><b>ALIAS-NAME&gt;</b>                                                                                                    | <p>The following parameters are recursive and common to the 'all', 'cluster-master', and 'rf-domain-manager' keywords:</p> <ul style="list-style-type: none"> <li>• <b>dns</b> - Configures DNS as the mode of monitoring critical resources. When configured, DNS message flows are used instead of ICMP or ARP packets to confirm critical resource availability.</li> <li>• <b>&lt;IP/HOST-ALIAS-NAME&gt;</b> - Configures the IPv4 address or host alias of the critical resource. Specify the IPv4 address or host alias name (should be existing and configured).</li> </ul>                                                                                                                                                                                     |
| <b>{dhcp vlan</b><br><b>{&lt;1-4094&gt;  </b><br><b>&lt;VLAN-ALIAS-</b><br><b>NAME&gt;]   dns &lt;IP/</b><br><b>HOST-ALIAS-</b><br><b>NAME&gt;}</b> | <p>The 'dhcp' and 'dns' parameters are recursive and you can optionally configure multiple VLANs and critical resource IPv4 addresses (or host alias names).</p> <ul style="list-style-type: none"> <li>• <b>dhcp</b> - Optional. Configures DHCP as the mode of monitoring critical resources. When configured, DHCP message flows (DHCP Discover, DHCP Offer, etc.) are used instead of ICMP or ARP packets to confirm critical resource availability.</li> <li>• <b>vlan [&lt;1-4094&gt; &lt;VLAN-ALIAS-NAME&gt;]</b> - Configures the VLAN on which the critical resource(s) is available. Specify the VLAN from 1 - 4094. Alternately, use a vlan-alias to identify the VLAN. If using a vlan-alias, ensure that the alias is existing and configured.</li> </ul> |
|                                                                                                                                                     | <ul style="list-style-type: none"> <li>• <b>dns</b> - Optional. Configures DNS as the mode of monitoring critical resources. When configured, DNS message flows are used instead of ICMP or ARP packets to confirm critical resource availability.</li> <li>• <b>&lt;IP/HOST-ALIAS-NAME&gt;</b> - Configures the IPv4 address or host alias of the critical resource. Specify the IPv4 address or host alias name (should be existing and configured).</li> </ul>                                                                                                                                                                                                                                                                                                      |

```
critical-resource monitor interval <5-86400>
```

|                                                   |                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>monitor interval</b><br><b>&lt;5-86400&gt;</b> | <p>Configures the critical resource monitoring frequency. This is the interval between two successive pings to the critical resource being monitored.</p> <ul style="list-style-type: none"> <li>• <b>&lt;5-86400&gt;</b> - Specifies the frequency in seconds. Specify the time from 5 - 86400 seconds. The default is 30 seconds.</li> </ul> |
|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
critical-resource retry-count <0-10>
```

|                                           |                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>retry-count</b><br><b>&lt;0-10&gt;</b> | <p>Configures the maximum number of failed attempts allowed to connect to a critical resource, using DHCP/DNS message flows, before marking it as down</p> <ul style="list-style-type: none"> <li>• <b>&lt;0-10&gt;</b> - Specifies the maximum number of retries from 0 - 10. The default value is 3 attempts.</li> </ul> |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Example

```
NOC-NX9500(config-profile-testNX9000)#critical-resource test monitor direct any
19.234.160.5 arp-only vlan 1
```

```

NOC-NX9500(config-profile-testNX9000)#show context include-factory | include cri
tical-resource
critical-resource monitor interval 30
service critical-resource port-mode-source-ip 0.0.0.0
critical-resource test monitor direct any 19.234.160.5 arp-only vlan 1
critical-resource retry-count 3
NOC-NX9500(config-profile-testNX9000)#

```

## crypto

[Profile Config Commands](#) on page 862

Use the `crypto` command to define a system-level local ID for Internet Security Association and Key Management Protocol (ISAKMP) negotiation and to enter the ISAKMP policy, ISAKMP client, or ISAKMP peer command set.

The following table summarizes `crypto` configuration mode commands:

| Command                                                        | Description                                                                      |
|----------------------------------------------------------------|----------------------------------------------------------------------------------|
| <a href="#">crypto</a> on page 931                             | Invokes commands used to configure ISAKMP policy, ISAKMP client, and ISAKMP peer |
| <a href="#">crypto-auto-ipsec-tunnel commands</a> on page 937  | Creates an auto IPsec VPN tunnel and enters its configuration mode               |
| <a href="#">crypto-ikev1/ikev2-policy commands</a> on page 943 | Creates a crypto IKEv1/IKEv2 policy and enters its configuration mode            |
| <a href="#">crypto-ikev1/ikev2-peer commands</a> on page 949   | Creates a IKEv1/IKEv2 peer and enters its configuration mode                     |
| <a href="#">crypto-map-config-commands</a> on page 955         | Creates a crypto map and enters its configuration mode                           |
| <a href="#">crypto-remote-vpn-client commands</a> on page 974  | Creates a remote VPN client and enters its configuration mode                    |

## crypto

[crypto](#) on page 931

Use the `crypto` command to define a system-level local ID for ISAKMP negotiation and enter the ISAKMP policy, ISAKMP client, or ISAKMP peer configuration mode.

A crypto map entry is a single policy that describes how certain traffic is secured. There are two types of crypto map entries: `ipsec-manual` and `ipsec-ike` entries. Each entry is given an index (used to sort the ordered list).

When a non-secured packet arrives on an interface, the crypto map associated with that interface is processed (in order). If a crypto map entry matches the non-secured traffic, the traffic is discarded.

When a packet is transmitted on an interface, the crypto map associated with that interface is processed. The first crypto map entry that matches the packet is used to secure the packet. If a suitable

Security Association (SA) exists, it is used for transmission. Otherwise, IKE is used to establish a SA with the peer. If no SA exists (and the crypto map entry is “respond only”), the packet is discarded.

When a secured packet arrives on an interface, its Security Parameter Index (SPI) is used to look up a SA. If a SA does not exist (or if the packet fails any of the security checks), it is discarded. If all checks pass, the packet is forwarded normally.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
crypto [auto-ipsec-secure|enable-ike-uniqueids|ike-version|ikev1|ikev2|ipsec|load-management|map|pki|plain-text-deny-acl-scope|remote-vpn-client]
```

```
crypto [auto-ipsec-secure|enable-ike-uniqueids|load-management]
```

```
crypto ike-version [ikev1-only|ikev2-only]
```

```
crypto ikev1 [dpd-keepalive <10-3600>|dpd-retries <1-100>|nat-keepalive <10-3600>|peer <IKEV1-PEER>|policy <IKEV1-POLICY-NAME>|remote-vpn]
```

```
crypto ikev2 [cookie-challenge-threshold <1-100>|dpd-keepalive <10-3600>|dpd-retries <1-100>|nat-keepalive <10-3600>|peer <IKEV2-PEER>|policy <IKEV2-POLICY-NAME>|remote-vpn]
```

```
crypto ipsec [df-bit|security-association|transform-set]
```

```
crypto ipsec df-bit [clear|copy|set]
```

```
crypto ipsec security-association lifetime [kilobytes <500-2147483646>|seconds <120-86400>]
```

```
crypto ipsec transform-set <TRANSFORM-SET-TAG> [esp-3des|esp-aes|esp-aes-192|esp-aes-256|esp-des|esp-null] [esp-aes-xcbc-mac|esp-md5-hmac|esp-sha-hmac|esp-sha256-hmac]
```

```
crypto map <CRYPTO-MAP-TAG> <1-1000> [ipsec-isakmp {dynamic}|ipsec-manual]
```

```
crypto pki import crl <TRUSTPOINT-NAME> URL <1-168>
```

```
crypto plain-text-deny-acl-scope [global|interface]
```

```
crypto remote-vpn-client
```

Parameters

```
crypto [auto-ipsec-secure|enable-ike-uniqueids|load-management]
```



|                             |                                                                                                                                                                       |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>auto-ipsec-secure</b>    | Configures the Auto IPsec Secure parameter settings. For Auto IPsec tunnel configuration commands, see <a href="#">crypto-auto-ipsec-tunnel commands</a> on page 937. |
| <b>enable-ike-uniqueids</b> | Enables Internet Key Exchange (IKE) unique ID check. For more information on IKE unique IDs, see <a href="#">remotegw</a> on page 941.                                |
| <b>load-management</b>      | Configures load management for platforms using software cryptography                                                                                                  |

```
crypto ike-version [ikev1-only|ikev2-only]
```

|                                                      |                                                                                                                                                                                                      |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ike-version</b><br><b>[ikev1-only ikev2-only]</b> | Selects and starts the IKE daemon <ul style="list-style-type: none"> <li>ikev1-only – Enables support for IKEv1 tunnels only</li> <li>ikev2-only – Enables support for IKEv2 tunnels only</li> </ul> |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
crypto ikev1 [dpd-keepalive <10-3600>|dpd-retries <1-100>|nat-keepalive <10-3600>|peer <IKEV1-PEER>|policy <IKEV1-POLICY-NAME>|remote-vpn]
```

|                                         |                                                                                                                                                                                                                                                                                       |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ikev1</b>                            | Configures the IKE version 1 parameters                                                                                                                                                                                                                                               |
| <b>dpd-keepalive &lt;10-3600&gt;</b>    | Sets the global Dead Peer Detection (DPD) keep alive interval from 10 - 3600 seconds. This is the interval between successive IKE keep alive messages sent to detect if a peer is dead or alive. The default is 30 seconds.                                                           |
| <b>dpd-retries &lt;1-1000&gt;</b>       | Sets the global DPD retries count from 1 - 1000. This is the number of keep alive messages sent to a peer before the tunnel connection is declared as dead. The default is 5.                                                                                                         |
| <b>nat-keepalive &lt;10-3600&gt;</b>    | Sets the global NAT keep alive interval from 10 - 3600 seconds. This is the interval between successive NAT keep alive messages sent to detect if a peer is dead or alive. The default is 20 seconds.                                                                                 |
| <b>peer &lt;IKEV1-PEER&gt;</b>          | Specify the name/Identifier for the IKEv1 peer. For IKEv1 peer configuration commands, see <a href="#">crypto-ikev1/ikev2-peer commands</a> on page 949.                                                                                                                              |
| <b>policy &lt;IKEV1-POLICY-NAME&gt;</b> | Configures an ISKAMP policy. Specify the name of the policy. The local IKE policy and the peer IKE policy must have matching group settings for successful negotiations. For IKEv1 policy configuration commands, see <a href="#">crypto-ikev1/ikev2-policy commands</a> on page 943. |
| <b>remote-vpn</b>                       | Specifies the IKEv1 remote-VPN server configuration (responder only)                                                                                                                                                                                                                  |

```
crypto ikev2 [cookie-challenge-threshold <1-100>|dpd-keepalive <10-3600>|dpd-retries <1-100>|nat-keepalive <10-3600>|peer <IKEV2-PEER>|policy <IKEV2-POLICY-NAME>|remote-vpn]
```

|                                                 |                                                                                                                                                            |
|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ikev2</b>                                    | Configures the IKE version 2 parameters                                                                                                                    |
| <b>cookie-challenge-threshold &lt;1-100&gt;</b> | Starts the cookie challenge mechanism after the number of half open IKE SAs exceeds the specified limit. Specify the limit from 1 - 100. The default is 5. |
| <b>dpd-keepalive &lt;10-3600&gt;</b>            | Sets the global DPD keepalive interval from 10 - 3600 seconds. The default is 30 seconds.                                                                  |
| <b>dpd-retries &lt;1-100&gt;</b>                | Sets the global DPD retries count from 1 - 100. The default is 5.                                                                                          |

|                                                |                                                                                                                                                                   |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>nat-keepalive</b><br><b>&lt;10-3600&gt;</b> | Sets the global NAT keepalive interval from 10 - 3600 seconds. The default is 20 seconds.                                                                         |
| <b>peer &lt;IKEV2-PEER&gt;</b>                 | Specify the name/Identifier for the IKEv2 peer                                                                                                                    |
| <b>policy &lt;IKEV2-POLICY-NAME&gt;</b>        | Configures an ISKAMP policy. Specify the policy name. The local IKE policy and the peer IKE policy must have matching group settings for successful negotiations. |
| <b>remote-vpn</b>                              | Specifies an IKEv2 remote-VPN server configuration (responder only)                                                                                               |

crypto ipsec df-bit [clear|copy|set]

|                                |                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipsec</b>                   | Configures the IPSec policy parameters                                                                                                                                                                                                                                                                                                                                                    |
| <b>df-bit [clear copy set]</b> | Configures Don't-Fragment (DF) bit handling for encapsulating header. The options are: <ul style="list-style-type: none"> <li>• clear - Clears the DF bit in the outer header and ignores in the inner header</li> <li>• copy - Copies the DF bit from the inner header to the outer header. This is the default setting.</li> <li>• set - Sets the DF bit in the outer header</li> </ul> |

crypto ipsec security-association lifetime [kilobytes <500-2147483646>|seconds <120-86400>]

|                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipsec</b>                         | Configures the IPSec policy parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>security-association</b>          | Configures the IPSec SAs parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>lifetime [kilobyte   seconds]</b> | Defines the IPSec SAs lifetime (in kilobytes and/or seconds). Values can be entered in both kilobytes and seconds, which ever limit is reached first, ends the SA. When the SA lifetime ends it is renegotiated as a security measure. <ul style="list-style-type: none"> <li>• kilobytes - Specifies a volume-based key duration (minimum is 500 KB and maximum is 2147483646 KB) <ul style="list-style-type: none"> <li>• &lt;500-2147483646&gt; - Specify a value from 500 - 2147483646 KB. The default is 4608000 KB.</li> </ul> </li> <li>• seconds - Specifies a time-based key duration (minimum is 120 seconds and maximum is 86400 seconds) <ul style="list-style-type: none"> <li>• &lt;120-86400&gt; - Specify a value from 120 - 86400 seconds. The default is 3600 seconds.</li> </ul> </li> </ul> <p>The security association lifetime can be overridden under crypto maps.</p> |

crypto ipsec transform-set <TRANSFORM-SET-TAG> [esp-3des|esp-aes|esp-aes-192| esp-aes-256| esp-des|esp-null] [esp-aes-xcbc-mac|esp-md5-hmac|esp-sha-hmac| esp-sha256-hmac]

|                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipsec</b>                                                                | Configures the IPsec policy parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>transform-set</b><br><b>&lt;TRANSFORM-SET-TAG&gt;</b>                    | <p>Defines the transform set configuration (authentication and encryption) for securing data. A transform set is a combination of security protocols, algorithms and other settings applied to IPsec protected traffic.</p> <ul style="list-style-type: none"> <li>• &lt;TRANSFORM-SET-TAG&gt; - Specify the transform set name.</li> </ul> <p>After specifying the transform set used by the IPsec transport connection, set the encryption method and the authentication scheme used with the transform set. The encryption methods are: DES, 3DES, AES, AES-192 and AES-256.</p> <p><b>Note:</b> The authentication schemes available are: esp-md5-hmac and esp-sha-hmac.</p> |
| <b>esp-3des</b>                                                             | Configures the ESP transform using 3DES cipher (168 bits). The transform set is assigned to a crypto map using the map's set > transform-set command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>esp-aes</b>                                                              | Configures the ESP transform using Advanced Encryption Standard (AES) cipher. The transform set is assigned to a crypto map using the map's set > transform-set command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>esp-aes-192</b>                                                          | Configures the ESP transform using AES cipher (192 bits). The transform set is assigned to a crypto map using the map's set > transform-set command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>esp-aes-256</b>                                                          | Configures the ESP transform using AES cipher (256 bits). The transform set is assigned to a crypto map using the map's set > transform-set command. This is the default setting.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>esp-des</b>                                                              | Configures the ESP transform using Data Encryption Standard (DES) cipher (56 bits). The transform set is assigned to a crypto map using the map's set > transform-set command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>esp-null</b>                                                             | Configures the ESP transform with no encryption                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>[ esp-aes-xcbc-mac   esp-md5-hmac   esp-sha-hmac   esp-sha256-hmac ]</b> | <p>The following keywords are common to all of the above listed transform sets. After specifying the transform set type, configure the authentication scheme used to validate identity credentials. The options are:</p> <ul style="list-style-type: none"> <li>• esp-aes-xcbc-mac - Configures ESP transform using AES-XCBC authorization</li> <li>• esp-md5-hmac - Configures ESP transform using HMAC-MD5 authorization</li> <li>• esp-sha-hmac - Configures ESP transform using HMAC-SHA authorization. This is the default setting.</li> <li>• esp-sha256-hmac - Configures ESP transform using HMAC-SHA256 authorization</li> </ul>                                        |

```
crypto map <CRYPTO-MAP-TAG> <1-1000> [ipsec-isakmp {dynamic}|ipsec-manual]
```

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>map &lt;CRYPTO-MAP-TAG&gt;</b> | <p>Configures the crypto map, a software configuration entity that selects data flows that require security processing. The crypto map also defines the policy for these data flows.</p> <ul style="list-style-type: none"> <li>• &lt;CRYPTO-MAP-TAG&gt; - Specify a name for the crypto map. The name should not exceed 32 characters. For crypto map configuration commands, see <a href="#">crypto-map-ipsec-manual-instance</a> on page 968.</li> </ul> |
| <b>&lt;1-1000&gt;</b>             | <p>Defines the crypto map entry sequence. Each crypto map uses a list of entries, each entry having a specific sequence number. Specifying multiple sequence numbers within the same crypto map provides the flexibility to connect to multiple peers from the same interface. Specify a value from 1 - 1000.</p>                                                                                                                                           |

|                                         |                                                                                                                                                                                                                 |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipsec-isakmp</b><br><b>{dynamic}</b> | Configures IPSEC w/ISAKMP. <ul style="list-style-type: none"> <li>dynamic - Optional. Configures dynamic map entry (remote VPN configuration) for XAUTH with mode-config or ipsec-l2tp configuration</li> </ul> |
| <b>ipsec-manual</b>                     | Configures IPSEC w/manual keying. Remote configuration is not allowed for manual crypto map.                                                                                                                    |

```
crypto pki import crl <TRUSTPOINT-NAME> <URL> <1-168>
```

|                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>pki</b>                                   | Configures certificate parameters. The Public Key Infrastructure (PKI) protocol creates encrypted public keys using digital certificates from certificate authorities.                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>import</b>                                | Imports a trustpoint related configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>crl</b><br><b>&lt;TRUSTPOINT-NAME&gt;</b> | Imports a Certificate Revocation List (CRL). Imports a trustpoint including either a private key and server certificate or a certificate authority (CA) certificate or both. A CRL is a list of revoked certificates that are no longer valid. A certificate can be revoked if the CA had improperly issued a certificate, or if a private-key is compromised. The most common reason for revocation is the user no longer being in sole possession of the private key. <ul style="list-style-type: none"> <li>&lt;TRUSTPOINT-NAME&gt; - Specify the trustpoint name.</li> </ul> |
| <b>&lt;URL&gt;</b>                           | Specify the CRL source address in the following format. Both IPv4 and IPv6 address formats are supported.<br>tftp://<hostname IPv4 or IPv6>[:port]/path/file<br>ftp://<user>:<passwd>@<hostname IPv4 or IPv6>[:port]/path/file<br>sftp://<user>:<passwd>@<hostname IPv4 or IPv6>[:port]/path/file<br>http://<hostname IPv4 or IPv6>[:port]/path/file<br>cf:/path/file<br>usb<n>:/path/file                                                                                                                                                                                       |
| <b>&lt;1-168&gt;</b>                         | Sets command replay duration from 1 - 168 hours. This is the interval (in hours) after which devices using this profile copy a CRL file from an external server and associate it with a trustpoint.                                                                                                                                                                                                                                                                                                                                                                              |

```
crypto plain-text-deny-acl-scope [global|interface]
```

|                                  |                                                                        |
|----------------------------------|------------------------------------------------------------------------|
| <b>plain-text-deny-acl-scope</b> | Configures plain-text-deny-acl-scope parameters                        |
| <b>global</b>                    | Applies the plain text deny ACL globally. This is the default setting. |
| <b>interface</b>                 | Applies the plain text deny ACL to the interface only                  |

```
crypto remote-vpn-client
```

|                          |                                                                                                                                 |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>remote-vpn-client</b> | Configures remote VPN client settings. For more information, see <a href="#">crypto-remote-vpn-client commands</a> on page 974. |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------|

#### Example

```
nx9500-6C8809(config-profile-default-rfs4000)#crypto ipsec transform-set tpsec-tag1 esp-
aes-256 esp-md5-hmac
nx9500-6C8809(config-profile-default-rfs4000)#crypto map map1 10 ipsec-isakmp dynamic
nx9500-6C8809(config-profile-default-rfs4000)#crypto plain-text-deny-acl-scope interface
```

```
nx9500-6C8809(config-profile-default-rfs4000)#show context
profile rfs4000 default-rfs4000
 bridge vlan 1
 tunnel-over-level2
```

```

ip igmp snooping
ip igmp snooping querier
no autoinstall configuration
no autoinstall firmware
device-upgrade persist-images
crypto ikev1 dpd-retries 1
crypto ikev1 policy ikev1-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ikev2 policy ikev2-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
crypto ipsec transform-set tpsec-tag1 esp-aes-256 esp-md5-hmac
crypto map map1 10 ipsec-isakmp dynamic
crypto ikev1 remote-vpn
crypto ikev2 remote-vpn
crypto auto-ipsec-secure
crypto plain-text-deny-acl-scope interface
interface radiol
interface radio2
interface up
nx9500-6C8809(config-profile-default-rfs4000)#

nx9500-6C8809(config-profile-default-rfs4000)#crypto ipsec transform-set tag1 esp-null esp-
md5-hmac

nx9500-6C8809(config-profile-default-rfs4000-transform-set-tag1)#?
Crypto Ipsec Configuration commands:
mode Encapsulation mode (transport/tunnel)
no Negate a command or set its defaults

clrscr Clears the display screen
commit Commit all changes made in this session
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

nx9500-6C8809(config-profile-default-rfs4000-transform-set-tag1)#

```

#### Related Commands

|                        |                                               |
|------------------------|-----------------------------------------------|
| <b>no</b> on page 1200 | Disables or reverts settings to their default |
|------------------------|-----------------------------------------------|

### crypto-auto-ipsec-tunnel commands

**crypto** on page 931

Creates an auto IPSec VPN tunnel and changes the mode to auto-ipsec-secure mode for further configuration

Auto IPSec tunneling provides a secure tunnel between two networked peer controllers or service platforms and associated access points that are within a range of valid IP addresses. You can define which packets are sent within the tunnel, and how they are protected. When a tunneled peer sees a sensitive packet, it creates a secure tunnel and sends the packet through the tunnel to its remote peer destination or associated access point.

Tunnels are sets of SA between two peers. SAs define the protocols and algorithms applied to sensitive packets and specify the keying mechanisms used by tunneled peers. SAs are unidirectional and exist in both the inbound and outbound direction. SAs are established per the rules and conditions of defined security protocols (AH or ESP).

The IKE protocol is a key management protocol used in conjunction with IPsec. IKE enhances IPsec by providing additional features, flexibility, and configuration simplicity for the IPsec standard. IKE enables secure communications without time consuming manual pre-configuration for auto IPsec tunneling.

```

nx9500-6C8809(config-profile-default-rfs4000)#crypto auto-ipsec-secure
nx9500-6C8809(config-profile-default-rfs4000-crypto-auto-ipsec-secure)#?
Crypto Auto IPSEC Tunnel commands:
 groupid Local/Remote identity and Authentication credentials for Auto
 IPsec Secure IKE negotiation
 ike-lifetime Set lifetime for ISAKMP security association
 ikev2 IKEv2 configuration commands
 ip Internet Protocol config commands
 no Negate a command or set its defaults
 remotegw Auto IPsec Secure Remote Peer IKE

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-profile-default-rfs4000-crypto-auto-ipsec-secure)#

```

The following table summarizes the crypto IPsec auto tunnel configuration mode commands:

| Command                                  | Description                                                                                                  |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| <a href="#">groupid</a> on page 938      | Specifies the identity string used for IKE authentication                                                    |
| <a href="#">ip</a> on page 939           | Enables the controller or service platform to uniquely identify APs and the hosts present in the AP's subnet |
| <a href="#">ike-lifetime</a> on page 940 | Configures the IKE SA's key lifetime in seconds                                                              |
| <a href="#">ikev2</a> on page 941        | Enables the forced re-authentication of IKEv2 peer                                                           |
| <a href="#">remotegw</a> on page 941     | Defines the IKE version used for an auto IPsec tunnel using secure gateways                                  |
| <a href="#">no</a> on page 942           | Removes or reverts the crypto auto IPsec tunnel settings                                                     |

groupid

[crypto-auto-ipsec-tunnel commands](#) on page 937

Specifies the identity string used for IKE authentication

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
groupid <WORD> [psk|rsa]
groupid <WORD> [psk [0 <WORD>|2 <WORD>|<WORD>]|rsa]
```

#### Parameters

```
groupid <WORD> [psk [0 <WORD>|2 <WORD>|<WORD>]|rsa]
```

|                                                              |                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;WORD&gt;</b>                                          | Specify a string not exceeding 64 characters. This is the group identity used for IKE exchange for auto IPsec secure peers. After providing a group ID, specify the authentication method used to authenticate peers on the auto IPsec secure tunnel. The options are: psk and rsa.                                                                             |
| <b>psk [0 &lt;WORD&gt;   2 &lt;WORD&gt;   &lt;WORD&gt; ]</b> | Configures the pre-shared key (PSK) as the authentication type for secure peer authentication on the auto IPsec secure tunnel <ul style="list-style-type: none"> <li>• 0 &lt;WORD&gt; - Configures a clear text key</li> <li>• 2 &lt;WORD&gt; - Configures an encrypted key</li> <li>• &lt;WORD&gt; - Specify a string value from 8 - 21 characters.</li> </ul> |
| <b>rsa</b>                                                   | Configures the Rivest-Shamir-Adleman (RSA) key. RSA is an algorithm for public key cryptography. It is the first algorithm known to be suitable for signing, as well as encryption. This is the default setting.                                                                                                                                                |



#### Note

Only one group ID is supported on the controller or service platform. All APs, controllers, and service platform must use the same group ID.

#### Example

```
nx9500-6C8809(config-profile-default-rfs4000-crypto-auto-ipsec-secure)#groupid
testgroup@123 rsa

nx9500-6C8809(config-profile-default-rfs4000-crypto-auto-ipsec-secure)#show context
crypto auto-ipsec-secure
groupid testgroup@123 rsa
nx9500-6C8809(config-profile-default-rfs4000-crypto-auto-ipsec-secure)#
```

ip

[crypto-auto-ipsec-tunnel commands](#) on page 937

Enables the controller to uniquely identify APs and the hosts present in the AP's subnet. This allows the controller to correctly identify the destination host and create a dynamic site-to-site VPN tunnel between the host and the private network behind the controller.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

## Syntax

`ip nat crypto`

## Parameters

`ip nat crypto`

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ip nat crypto</b> | Enables unique identification of APs and the hosts present in each AP's subnet. Providing a unique ID enables the access point, wireless controller, or service platform to uniquely identify the destination device. This is essential in networks where there are multiple APs behind a router, or when two (or more) APs behind two (or more) different routers have the same IP address. Further, the same subnet exists behind these APs. For example, let us consider a scenario where there are two APs (A and B) behind two routers (1 and 2). AP 'A' is behind router '1'. And AP 'B' is behind router '2'. Both these APs have the same IP address (192.168.13.8). The subnet behind APs A and B is also the same (100.1.1.0/24). In such a scenario the controller fails to uniquely identify the hosts present in either AP's subnet. For more information, see <a href="#">remotegw</a> on page 941 and <a href="#">crypto</a> on page 931. |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Example

```
rfs4000-229D58config-profile-testRFS4000-crypto-auto-ipsec-secure)#ip nat crypto

rfs4000-229D58config-profile-testRFS4000-crypto-auto-ipsec-secure)#show context
crypto auto-ipsec-secure
 remotegw ike-version ikev2 uniqueid
 ip nat crypto
rfs4000-229D58config-profile-testRFS4000-crypto-auto-ipsec-secure)#
```

ike-lifetime

[crypto-auto-ipsec-tunnel commands](#) on page 937

Configures the IKE SA's key lifetime in seconds

The lifetime defines how long a connection (encryption/authentication keys) should last, from successful key negotiation to expiration. Two peers need not exactly agree on the lifetime, though if they do not, there is some clutter for a superseded connection on the peer defining the lifetime as longer.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

## Syntax

`ike-lifetime <600-86400>`

## Parameters

`ike-lifetime <600-86400>`

|                                                 |                                                                                                                                                                                        |
|-------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ike-lifetime</b><br><b>&lt;600-86400&gt;</b> | Sets the IKE SA's key lifetime in seconds <ul style="list-style-type: none"><li>• &lt;600-86400&gt; – Specify a value from 600 - 86400 seconds. The default is 8600 seconds.</li></ul> |
|-------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



### Example

```
rfs4000-229D58(config-profile-testRFS4000-crypto-auto-ipsec-secure)#ike-lifetime 800

rfs4000-229D58(config-profile-testRFS4000-crypto-auto-ipsec-secure)#show context crypto
auto-ipsec-secure
 ike-lifetime 800
rfs4000-229D58(config-profile-testRFS4000-crypto-auto-ipsec-secure)#
```

ikev2

[crypto-auto-ipsec-tunnel commands](#) on page 937

Enables the forced IKEv2 peer re-authentication. This option is disabled by default.

In most IPsec tunnel configurations, the lifetime of IKE SAs between peers is limited. Once the IKE SA key expires it is renegotiated. In such a scenario, the IKEv2 tunnel peers may or may not re-authenticate themselves. When enabled, IKE tunnel peers have to re-authenticate each time the IKE SA is renegotiated.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
ikev2 peer reauth
```

### Parameters

```
ikev2 peer reauth
```

|                          |                                                                                                                                           |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ikev2 peer reauth</b> | Enables IKEv2 peer re-authentication. When enabled, IKE tunnel peers are forced to re-authenticate each time the IKE key is renegotiated. |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|

### Example

```
rfs4000-229D58(config-profile-testRFS4000-crypto-auto-ipsec-secure)#ikev2 peer reauth
```

remotegw

[crypto-auto-ipsec-tunnel commands](#) on page 937

Defines the IKE version used for auto IPSEC tunnel negotiation with the IPsec remote gateway other than the controller

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
remotegw ike-version [ikev1-aggr|ikev1-main|ikev2] {uniqueid}
```

### Parameters

```
remotegw ike-version [ikev1-aggr|ikev1-main|ikev2] {uniqueid}
```

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>remotegw ike-version</b> | Configures the IKE version used for initiating auto IPsec tunnel with secure gateways other than the controller                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>ikev1-aggr</b>           | Aggregation mode is used by the auto IPsec tunnel initiator to set up the connection                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>ikev1-main</b>           | Main mode is used by the auto IPsec tunnel initiator to establish the connection                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>ikev2</b>                | IKEv2 is the preferred method when wireless controller/AP only is used                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>uniqueid</b>             | <p>This keyword is common to all of the above parameters.</p> <ul style="list-style-type: none"> <li>• <b>uniqueid</b> – Optional. Enables the assigning of a unique ID to APs (using this profile) behind a router by prefixing the MAC address to the group ID</li> </ul> <p>Providing a unique ID enables the access point, wireless controller, or service platform to uniquely identify the destination device. This is essential in networks where there are multiple APs behind a router, or when two (or more) APs behind two (or more) different routers have the same IP address. For example, let us consider a scenario where there are two APs (A and B) behind two routers (1 and 2). AP 'A' is behind router '1'. And AP 'B' is behind router '2'. Both these APs have the same IP address (192.168.13.8). In such a scenario, the controller fails to establish an Auto IPsec VPN tunnel to either APs, because it is unable to uniquely identify them.</p> <p>After enabling unique ID assignment, enable IKE unique ID check. For more information, see <a href="#">crypto</a> on page 931.</p> |

#### Example

```
nx9500-6C8809(config-profile-default-rfs4000-crypto-auto-ipsec-secure)#remotegw
ike-version ikev2 uniqueid
```

```
nx9500-6C8809(config-profile-default-rfs4000-crypto-auto-ipsec-secure)#show context
```

```
crypto auto-ipsec-secure
remotegw ike-version ikev2 uniqueid
nx9500-6C8809(config-profile-default-rfs4000-crypto-auto-ipsec-secure)#
```

no

[crypto-auto-ipsec-tunnel commands](#) on page 937

Removes or resets this auto IPsec tunnel settings

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
no [groupid|ike-lifetime|ikev2 peer reauth|ip nat crypto]
```

#### Parameters

```
no <PARAMETERS>
```

|                                        |                                                                                    |
|----------------------------------------|------------------------------------------------------------------------------------|
| <b>no</b><br><b>&lt;PARAMETERS&gt;</b> | Removes or resets this auto IPsec tunnel's settings based on the parameters passed |
|----------------------------------------|------------------------------------------------------------------------------------|

#### Example

The following example shows the Auto IPsec VLAN bridge settings before the 'no' command is executed:

```
nx9500-6C8809(config-profile-default-rfs4000-crypto-auto-ipsec-secure)#show context
crypto auto-ipsec-secure
 groupid testpassword@123 rsa
nx9500-6C8809(config-profile-default-rfs4000-crypto-auto-ipsec-secure)#
```

```
nx9500-6C8809(config-profile-default-rfs4000-crypto-auto-ipsec-secure)#no groupid
```

The following example shows the Auto IPsec VLAN bridge settings after the 'no' command is executed:

```
nx9500-6C8809(config-profile-default-rfs4000-crypto-auto-ipsec-secure)#show context
crypto auto-ipsec-secure
nx9500-6C8809(config-profile-default-rfs4000-crypto-auto-ipsec-secure)#
```

## crypto-ikev1/ikev2-policy commands

[crypto](#) on page 931

Defines crypto-IKEv1/IKEv2 commands in detail

IKE protocol is a key management protocol standard used in conjunction with IPsec. IKE enhances IPsec by providing additional features, flexibility, and configuration simplicity for the IPsec standard. IKE automatically negotiates IPsec SAs and enables secure communications without time consuming manual pre-configuration.

Use the (config) instance to configure IKEv1/IKEv2 policy configuration commands.

To navigate to the IKEv1/IKEv2 policy config instance, use the following commands:

```
<DEVICE>(config)#profile <DEVICE-TYPE> <PROFILE-NAME>
<DEVICE>(config-profile-<PROFILE-NAME>)#crypto ikev1/ikev2 policy <IKEV1/IKEV2-POLICY-NAME>
```

```
nx9500-6C8809(config-profile-default-rfs4000)#crypto ikev1 policy ikev1-testpolicy
rfs7000-37FABE(config-profile-default-rfs4000-ikev1-policy-ikev1-testpolicy)#?
```

Crypto IKEv1 Policy Configuration commands:

|                 |                                                   |
|-----------------|---------------------------------------------------|
| dpd-keepalive   | Set Dead Peer Detection interval in seconds       |
| dpd-retries     | Set Dead Peer Detection retries count             |
| isakmp-proposal | Configure ISAKMP Proposals                        |
| lifetime        | Set lifetime for ISAKMP security association      |
| mode            | IKEv1 mode (main/aggressive)                      |
| no              | Negate a command or set its defaults              |
| clrscr          | Clears the display screen                         |
| commit          | Commit all changes made in this session           |
| end             | End current mode and change to EXEC mode          |
| exit            | End current mode and down to previous mode        |
| help            | Description of the interactive help system        |
| revert          | Revert changes                                    |
| service         | Service Commands                                  |
| show            | Show running system information                   |
| write           | Write running configuration to memory or terminal |

```
nx9500-6C8809(config-profile-default-rfs4000-ikev1-policy-ikev1-testpolicy)#
```

```
nx9500-6C8809(config-profile-test-ikev2-policy-ikev2-testpolicy)#?
```

Crypto IKEv2 Policy Configuration commands:

|                 |                                                            |
|-----------------|------------------------------------------------------------|
| dpd-keepalive   | Set Dead Peer Detection interval in seconds                |
| isakmp-proposal | Configure ISAKMP Proposals                                 |
| lifetime        | Set lifetime for ISAKMP security association               |
| no              | Negate a command or set its defaults                       |
| sa-per-acl      | Setup single SA for all rules in the ACL (ONLY APPLICABLE) |

FOR SITE-TO-SITE VPN)

```
clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal
```

```
nx9500-6C8809(config-profile-test-ikev2-policy-ikev2-testpolicy)#
```



#### Note

IKEv2 being an improved version of the original IKEv1 design, is recommended in most deployments. IKEv2 provides enhanced cryptographic mechanisms, NAT and firewall traversal, attack resistance, etc.

The following table summarizes crypto IKEv1/iKEv2 configuration mode commands:

| Command                                     | Description                                                                                                  |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| <a href="#">dpd-keepalive</a> on page 944   | Sets DPD keep alive packet interval                                                                          |
| <a href="#">dpd-retries</a> on page 945     | Sets the maximum number of attempts for sending DPD keep alive packets (applicable only to the IKEv1 policy) |
| <a href="#">isakmp-proposal</a> on page 945 | Configures ISAKMP proposals                                                                                  |
| <a href="#">lifetime</a> on page 946        | Specifies how long an IKE SA is valid before it expires                                                      |
| <a href="#">mode</a> on page 947            | Sets the mode of the tunnels (applicable only to the IKEv1 policy)                                           |
| <a href="#">no</a> on page 948              | Removes or reverts IKEv1/IKEv2 policy settings                                                               |

#### dpd-keepalive

[crypto-ikev1/ikev2-policy commands](#) on page 943

Sets the DPD keep-alive packet interval

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
dpd-keepalive <10-3600>
```

Parameters

```
dpd-keepalive <10-3600>
```

**<10-3600>**

Specifies the interval, in seconds, between successive DPD keep alive packets. The IKE keep alive message is used to detect a dead peer on the remote end of the IPsec VPN tunnel. Specify the time from 10 - 3600 seconds. The default is 30 seconds.

#### Example

```
nx9500-6C8809(config-profile-default-rfs4000-ikev1-policy-ikev1-testpolicy)#dpd-keepalive 11
```

```
nx9500-6C8809(config-profile-default-rfs4000-ikev1-policy-testpolicy)#show context
crypto ikev1 policy testpolicy
 dpd-keepalive 11
 isakmp-proposal default encryption aes-256 group 2 hash sha
nx9500-6C8809(config-profile-default-rfs4000-ikev1-policy-testpolicy)#
```

dpd-retries

[crypto-ikev1/ikev2-policy commands](#) on page 943

Sets the maximum number of times DPD keep-alive packets are sent to a peer. Once this value is exceeded, without a response from the peer, the VPN tunnel connection is declared dead. This option is available only for the IKEv1 policy.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
dpd-retries <1-100>
```

#### Parameters

```
dpd-retries <1-100>
```

**<1-100>**

Declares a peer dead after the specified number of retries. Specify a value from 1 - 100. The default is 5.

#### Example

```
nx9500-6C8809(config-profile-default-rfs4000-ikev1-policy-ikev1-testpolicy)#dpd-retries 10
```

```
nx9500-6C8809(config-profile-default-rfs4000-ikev1-policy-ikev1-testpolicy)#show context
crypto ikev1 policy testpolicy
 dpd-keepalive 11
 dpd-retries 10
 isakmp-proposal default encryption aes-256 group 2 hash sha
nx9500-6C8809(config-profile-default-rfs4000-ikev1-policy-ikev1-testpolicy)#
```

isakmp-proposal

[crypto-ikev1/ikev2-policy commands](#) on page 943

Configures ISAKMP proposals and their parameters

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000

- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
isakmp-proposal <WORD> encryption [3des|aes|aes-192|aes-256] group [14|2|5] hash [aes-xcbc-mac|md5|sha|sha256]
```

#### Parameters

```
isakmp-proposal <WORD> encryption [3des|aes|aes-192|aes-256] group [14|2|5] hash [aes-xcbc-mac|md5|sha|sha256]
```

|                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;WORD&gt;</b>                          | Assigns the target peer (tunnel destination) a 32 character maximum name to distinguish it from others with a similar configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>encryption [3des aes aes-192 aes-256]</b> | Configures the encryption method used by the tunneled peers to securely inter-operate <ul style="list-style-type: none"> <li>• 3des - Configures triple data encryption standard</li> <li>• aes - Configures AES (128 bit keys)</li> <li>• aes-192 - Configures AES (192 bit keys)</li> <li>• aes-256 - Configures AES (256 bit keys). This is the default setting.</li> </ul>                                                                                                                                                                                                           |
| <b>group [14 2 5]</b>                        | Specifies the Diffie-Hellman (DH) group identifier used by VPN peers to derive a shared secret password without having to transmit. DH groups determine the strength of the key used in key exchanges. The higher the group number, the stronger and more secure the key. Options include 2, 5 and 14. <ul style="list-style-type: none"> <li>• 14 - Configures DH group 14</li> <li>• 2 - Configures DH group 2. This is the default setting.</li> <li>• 5 - Configures DH group 5</li> </ul>                                                                                           |
| <b>hash [aes-xcbc-mac md5 sha sha256]</b>    | Specifies the hash algorithm used to authenticate data transmitted over the IKE SA. The hash algorithm specified here is used by VPN peers to exchange credential information. <ul style="list-style-type: none"> <li>• aes-xcbc-mac - Uses AES XCBC Auth hash algorithm. This option is applicable only to the IKEv2 policy configuration context.</li> <li>• md5 - Uses Message Digest 5 (MD5) hash algorithm</li> <li>• sha - Uses Secure Hash Authentication (SHA) hash algorithm. This is the default setting.</li> <li>• sha256 - Uses Secure Hash Standard 2 algorithm</li> </ul> |

#### Example

```
nx9500-6C8809(config-profile-default-rfs4000-ikev1-policy-ikev1-testpolicy)#isakmp-proposal testproposal encryption aes group 2 hash sha
```

```
nx9500-6C8809(config-profile-default-rfs4000-ikev1-policy-ikev1-testpolicy)#show context
crypto ikev1 policy testpolicy
 dpd-keepalive 11
 dpd-retries 10
 isakmp-proposal default encryption aes-256 group 2 hash sha
 isakmp-proposal testpraposal encryption aes group 2 hash sha
nx9500-6C8809(config-profile-default-rfs4000-ikev1-policy-ikev1-testpolicy)#
```

lifetime

[crypto-ikev1/ikev2-policy commands](#) on page 943

Specifies how long an IKE SA (encryption/authentication keys) is valid. The value specified is the validity period of the IKE SA from successful key negotiation to expiration.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

**lifetime** <600-86400>

#### Parameters

lifetime <600-86400>

|                                             |                                                                                                                                                                                                                                                          |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>lifetime</b><br><b>&lt;600-86400&gt;</b> | Specifies how many seconds an IKE SA lasts before it expires. Set a time stamp from 600 - 86400 seconds. <ul style="list-style-type: none"> <li>• &lt;600-86400&gt; - Specify a value from 600 - 86400 seconds. The default is 86400 seconds.</li> </ul> |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Example

```

nx9500-6C8809(config-profile-default-rfs4000-ikev1-policy-ikev1-testpolicy)#lifetime 655

nx9500-6C8809(config-profile-default-rfs4000-ikev1-policy-ikev1-testpolicy)#show context
crypto ikev1 policy testpolicy
 dpd-keepalive 11
 dpd-retries 10
 lifetime 655
 isakmp-proposal default encryption aes-256 group 2 hash sha
 isakmp-proposal testproposal encryption aes group 2 hash sha
nx9500-6C8809(config-profile-default-rfs4000-ikev1-policy-ikev1-testpolicy)#

```

mode

[crypto-ikev1/ikev2-policy commands](#) on page 943

Configures the IPSec mode of operation for the IKEv1 policy. This option is not available for IKEv2 policy.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

**mode** [aggressive|main]

#### Parameters

mode [aggressive|main]

|                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mode</b><br><b>[aggressive </b><br><b>main]</b> | Sets the mode of the tunnels <ul style="list-style-type: none"> <li>• aggressive - Initiates the aggressive mode</li> <li>• main - Initiates the main mode</li> </ul> <p>If configuring the IKEv1 IPSec policy, define the IKE mode as either main or aggressive. In the aggressive mode, 3 messages are exchanged between the IPSec peers to setup the SA. On the other hand, in the main mode, 6 messages are exchanged. The default setting is main.</p> |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Example

```
nx9500-6C8809(config-profile-default-rfs4000-ikev1-policy-ikev1-testpolicy)#mode aggressive

nx9500-6C8809(config-profile-default-rfs4000-ikev1-policy-ikev1-testpolicy)#show context
crypto ikev1 policy testpolicy
 dpd-keepalive 11
 dpd-retries 10
 lifetime 655
 isakmp-proposal default encryption aes-256 group 2 hash sha
 isakmp-proposal testpraposal encryption aes group 2 hash sha
 mode aggressive
nx9500-6C8809(config-profile-default-rfs4000-ikev1-policy-ikev1-testpolicy)#
```

no

[crypto-ikev1/ikev2-policy commands](#) on page 943

Removes or reverts IKEv1/IKEv2 policy settings

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

## Syntax

```
no [dpd-keepalive|dpd-retries|isakmp-proposal <WORD>|lifetime|mode]
```

## Parameters

```
no <PARAMETERS>
```

|                                                                                                             |
|-------------------------------------------------------------------------------------------------------------|
| <b>no &lt;PARAMETERS&gt;</b> Removes or reverts this IKEv1/IKEv2 policy settings based on parameters passed |
|-------------------------------------------------------------------------------------------------------------|

## Example

The following example shows the IKEV1 Policy settings before the 'no' commands are executed:

```
nx9500-6C8809(config-profile-default-rfs4000-ikev1-policy-ikev1-testpolicy)#show context
crypto ikev1 policy testpolicy
 dpd-keepalive 11
 dpd-retries 10
 lifetime 655
 isakmp-proposal default encryption aes-256 group 2 hash sha
 isakmp-proposal testpraposal encryption aes group 2 hash sha
 mode aggressive
nx9500-6C8809(config-profile-default-rfs4000-ikev1-policy-ikev1-testpolicy)#

nx9500-6C8809(config-profile-default-rfs4000-ikev1-policy-ikev1-testpolicy)#no mode
nx9500-6C8809(config-profile-default-rfs4000-ikev1-policy-ikev1-testpolicy)#no dpd-keepalive
nx9500-6C8809(config-profile-default-rfs4000-ikev1-policy-ikev1-testpolicy)#no dpd-retries
```

The following example shows the IKEV1 Policy settings after the 'no' commands are executed:

```
nx9500-6C8809(config-profile-default-rfs4000-ikev1-policy-ikev1-testpolicy)# show context
crypto ikev1 policy testpolicy
 lifetime 655
 isakmp-proposal default encryption aes-256 group 2 hash sha
 isakmp-proposal testpraposal encryption aes group 2 hash sha
nx9500-6C8809(config-profile-default-rfs4000-ikev1-policy-ikev1-testpolicy)#
```



## crypto-ikev1/ikev2-peer commands

[crypto](#) on page 931

Use the (config) instance to configure IKEv1/IKEv2 peer configuration commands. To navigate to the IKEv1/IKEv2 peer config instance, use the following commands:

```
<DEVICE>(config)#profile <DEVICE-TYPE> <PROFILE-NAME>
<DEVICE>(config-profile-<PROFILE-NAME>)#crypto ikev1/ikev2 peer <IKEV1/IKEV2-PEER-NAME>
```

```
nx9500-6C8809(config-profile-default-rfs4000)#crypto ikev1 peer peer1
nx9500-6C8809(config-profile-default-rfs4000-ikev1-peer-peer1)#?
```

Crypto IKEV1 Peer Configuration commands:

```
authentication Configure Authentication credentials
ip Configure peer address/fqdn
localid Set local identity
no Negate a command or set its defaults
remoteid Configure remote peer identity
use Set setting to use

clrscr Clears the display screen
commit Commit all changes made in this session
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal
```

```
nx9500-6C8809(config-profile-default-rfs4000-ikev1-peer-peer1)#
```

```
nx9500-6C8809(config-profile-default-rfs4000)#crypto ikev2 peer peer1
nx9500-6C8809(config-profile-default-rfs4000-ikev2-peer-peer1)#?
```

Crypto IKEV2 Peer Configuration commands:

```
authentication Configure Authentication credentials
ip Configure peer address/fqdn
localid Set local identity
no Negate a command or set its defaults
remoteid Configure remote peer identity
use Set setting to use

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal
```

```
nx9500-6C8809(config-profile-default-rfs4000-ikev2-peer-peer1)#
```

The following table summarizes crypto IPsec IKEv1/IKEv2 peer configuration mode commands:

| Command                                    | Description                                                    |
|--------------------------------------------|----------------------------------------------------------------|
| <a href="#">authentication</a> on page 950 | Configures a peer's authentication mode and the pre-shared key |
| <a href="#">ip</a> on page 951             | Configures the peer's IP address                               |

| Command                           | Description                                                                                                                                                              |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>localid</code> on page 951  | Configures a peer's local identity details                                                                                                                               |
| <code>remoteid</code> on page 952 | Configures a remote peer's identity details                                                                                                                              |
| <code>use</code> on page 953      | Associates an IKEv1 policy and IKEv2 policy with the IKEv1 and IKEv2 peer respectively                                                                                   |
| <code>no</code> on page 954       | Negates a command or reverts settings to their default. The <code>no</code> command, when used in the ISAKMP policy mode, defaults the ISAKMP protection suite settings. |

authentication

`crypto-ikev1/ikev2-peer commands` on page 949

Configures IKEv1/IKEv2 peer's authentication mode and the pre-shared key

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
authentication [psk|rsa]
```

```
authentication psk [0 <WORD>|2 <WORD>|<WORD>] {local|remote}
```

```
authentication rsa
```

Parameters

```
authentication psk [0 <WORD>|2 <WORD>|<WORD>] {local|remote}
```

|                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>psk [0 &lt;WORD&gt;  2 &lt;WORD&gt;  &lt;WORD&gt;] {local remote}</pre> | <p>Configures the authentication mode as pre-shared key (PSK). The PSK is a string, 8 - 12 characters long. It is shared by both ends of the VPN tunnel connection. If using IKEv2, both a local and remote string must be specified for handshake validation at both ends (local and remote) of the VPN connection.</p> <ul style="list-style-type: none"> <li>• 0 &lt;WORD&gt; - Configures a clear text key</li> <li>• 2 &lt;WORD&gt; - Configures an encrypted key</li> <li>• &lt;WORD&gt; - Configures the pre-shared key</li> </ul> <p>The following keywords are available only in the IKEv2 peer configuration mode:</p> <ul style="list-style-type: none"> <li>• local - Optional. Uses the specified key for local peer authentication only</li> <li>• remote - Optional. Uses the specified key for remote peer authentication only</li> </ul> <p><b>Note:</b> In case the peer type is not specified, this string is used for authenticating both local and remote peers.</p> |
|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
authentication rsa
```

|            |                                                                                                                                                                                                                                                                                                                                                                      |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>rsa</b> | Configures the authentication mode as Rivest, Shamir, and Adleman (RSA) This is the default setting (for both IKEv1 and IKEv2). RSA is the first known public-key cryptography algorithm designed signing and encryption. If configuring the IKEv2 peer, the 'rsa' option allows you to enable authentication at both ends of the VPN connection (local and remote). |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Example

```

nx9500-6C8809(config-profile-default-rfs4000-ikev1-peer-peer1)#authentication rsa

nx9500-6C8809(config-profile-default-rfs4000-ikev2-peer-peer1)#authentication
psk 0 key@123456

nx9500-6C8809(config-profile-default-rfs4000-ikev2-peer-peer1)#show context
crypto ikev2 peer peer1
 authentication psk 0 key@123456 local
 authentication psk 0 key@123456 remote
nx9500-6C8809(config-profile-default-rfs4000-ikev2-peer-peer1)#

```

ip

[crypto-ikev1/ikev2-peer commands](#) on page 949

Sets the IP address or Fully Qualified Domain Name (FQDN) of the IPSec VPN peer used in the tunnel setup

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
ip [address <IP>|fqdn <WORD>]
```

#### Parameters

```
ip [address <IP>|fqdn <WORD>]
```

|                           |                                          |
|---------------------------|------------------------------------------|
| <b>address &lt;IP&gt;</b> | Specify the peer device's IP address.    |
| <b>fqdn &lt;WORD&gt;</b>  | Specify the peer device's FQDN hostname. |

#### Example

```

nx9500-6C8809(config-profile-default-rfs4000-ikev1-peer-peer1)#ip address 172.16.10.12

nx9500-6C8809(config-profile-default-rfs4000-ikev1-peer-peer1)#show context
crypto ikev1 peer peer1
 ip address 172.16.10.12
nx9500-6C8809(config-profile-default-rfs4000-ikev1-peer-peer1)#

nx9500-6C8809(config-profile-default-rfs4000-ikev2-peer-peer1)#ip address 192.168.10.6

nx9500-6C8809(config-profile-default-rfs4000-ikev2-peer-peer1)#show context
crypto ikev2 peer peer1
 ip address 192.168.10.6
 authentication psk 0 test@123456 local
 authentication psk 0 test@123456 remote
nx9500-6C8809(config-profile-default-rfs4000-ikev2-peer-peer1)#

```

localid

[crypto-ikev1/ikev2-peer commands](#) on page 949

Sets a IKEv1/IKEv2 peer's local identity. This local identifier is used with this peer configuration for an IKE exchange with the target VPN IPsec peer.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
localid [address | autogen-uniqueid | dn | email | fqdn | string]
```

```
localid [address <IP> | autogen-uniqueid <WORD> | dn <WORD> | email <WORD> | fqdn <WORD> | string <WORD>]
```

Parameters

```
localid [address <IP> | dn <WORD> | email <WORD> | fqdn <WORD> | string <WORD>]
```

|                                      |                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>address &lt;IP&gt;</b>            | Configures the peer's IP address. The IP address is used as local identity.                                                                                                                                                                                                                                                                                                                                  |
| <b>autogen-uniqueid &lt;WORD&gt;</b> | Generates a localid using the device's unique identity. The system prefixes the device's unique identity to the string provided here. The device's unique identity should be existing and configured. For more information on configuring a device's unique identity, see <a href="#">autogen-uniqueid</a> on page 883. <ul style="list-style-type: none"><li>• &lt;WORD&gt; - Provide the string.</li></ul> |
| <b>dn &lt;WORD&gt;</b>               | Configures the peer's distinguished name. (for example, "C=us ST=<state> L=<location> O=<organization> OU=<org unit>". The maximum length is 128 characters.                                                                                                                                                                                                                                                 |
| <b>email &lt;WORD&gt;</b>            | Configures the peer's e-mail address. The maximum length is 128 characters.                                                                                                                                                                                                                                                                                                                                  |
| <b>fqdn &lt;WORD&gt;</b>             | Configures the peer's FQDN. The maximum length is 128 characters.                                                                                                                                                                                                                                                                                                                                            |
| <b>string &lt;WORD&gt;</b>           | Configures the peer's identity string. The maximum length is 128 characters. This is the default setting.                                                                                                                                                                                                                                                                                                    |

Example

```
nx9500-6C8809(config-profile-default-rfs4000-ikev1-peer-peer1)#localid email bob@examplecompany.com
```

```
nx9500-6C8809(config-profile-default-rfs4000-ikev1-peer-peer1)#show context crypto ikev1 peer peer1 ip address 172.16.10.12 localid email bob@examplecompany.com nx9500-6C8809(config-profile-default-rfs4000-ikev1-peer-peer1)#
```

remoteid

[crypto-ikev1/ikev2-peer commands](#) on page 949

Configures a IKEv1/IKEv2 peer's remote identity. This remote identifier is used with this peer configuration for an IKE exchange with the target VPN IPsec peer.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
remoteid [address <IP>|dn <WORD>|email <WORD>|fqdn <WORD>|string <WORD>]
```

#### Parameters

```
remoteid [address <IP>|dn <WORD>|email <WORD>|fqdn <WORD>|string <WORD>]
```

|                            |                                                                                                                                                                    |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>address &lt;IP&gt;</b>  | Configures the remote IKEv1/IKEv2 peer's IP address. The IP address is used as the peer's remote identity.                                                         |
| <b>dn &lt;WORD&gt;</b>     | Configures the remote peer's distinguished name. For example, "C=us ST=<state> L=<location> O=<organization> OU=<org unit>". The maximum length is 128 characters. |
| <b>email &lt;WORD&gt;</b>  | Configures the remote peer's e-mail address. The maximum length is 128 characters.                                                                                 |
| <b>fqdn &lt;WORD&gt;</b>   | Configures a peer's FQDN. The maximum length is 128 characters.                                                                                                    |
| <b>string &lt;WORD&gt;</b> | Configures a peer's identity string. The maximum length is 128 characters.                                                                                         |

#### Example

```
nx9500-6C8809(config-profile-default-rfs4000-ikev1-peer-peer1)#remoteid dn SanJose
```

```
nx9500-6C8809(config-profile-default-rfs4000-ikev1-peer-peer1)#show context
```

```
crypto ikev1 peer peer1
 ip address 172.16.10.12
 remoteid dn SanJose
 localid email bob@examplecompany.com
```

```
nx9500-6C8809(config-profile-default-rfs4000-ikev1-peer-peer1)#
```

```
nx9500-6C8809(config-profile-default-rfs4000-ikev1-peer-peer1)#remoteid address
157.235.209.63
```

```
nx9500-6C8809(config-profile-default-rfs4000-ikev2-peer-peer1)#show context
```

```
crypto ikev2 peer peer1
 remoteid address 157.235.209.63
```

```
nx9500-6C8809(config-profile-default-rfs4000-ikev2-peer-peer1)#
```

use

[crypto-ikev1/ikev2-peer commands](#) on page 949

Associates IKEv1/IKEv2 policy with the IKEv1/IKEv2 peer respectively

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
use ikev1-policy <IKEV1-POLICY-NAME>
```

```
use ikev2-policy <IKEV2-POLICY-NAME>
```

## Parameters

use ikev1-policy <IKEV1-POLICY-NAME>

|                                                   |                                                                                                                                                   |
|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>use ikev1-policy &lt;IKEV1-POLICY-NAME&gt;</b> | Specify the IKEv1 policy name.<br>The local IKEv1 policy and the peer IKEv1 policy must have matching group settings for successful negotiations. |
|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|

use ikev2-policy <IKEV2-POLICY-NAME>

|                                                   |                                                                                                                                                   |
|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>use ikev2-policy &lt;IKEV2-POLICY-NAME&gt;</b> | Specify the IKEv2 policy name.<br>The local IKEv2 policy and the peer IKEv2 policy must have matching group settings for successful negotiations. |
|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|

## Example

```
nx9500-6C8809(config-profile-default-rfs4000-ikev1-peer-peer1)#use ikev1-policy test-ikev1policy
```

```
nx9500-6C8809(config-profile-default-rfs4000-ikev1-peer-peer1)#show context
crypto ikev1 peer peer1
 ip address 172.16.10.12
 remoteid dn SanJose
 localid email bob@examplecompany.com
 use ikev1-policy test-ikev1policy
nx9500-6C8809(config-profile-default-rfs4000-ikev1-peer-peer1)#
```

```
nx9500-6C8809(config-profile-default-rfs4000-ikev2-peer-peer1)#use ikev2-policy test-ikev2policy
```

```
nx9500-6C8809(config-profile-default-rfs4000-ikev2-peer-peer1)#show context
crypto ikev2 peer peer1
 remoteid address 157.235.209.63
 use ikev2-policy test-ikev2policy
nx9500-6C8809(config-profile-default-rfs4000-ikev2-peer-peer1)#
```

no

[crypto-ikev1/ikev2-peer commands](#) on page 949

Removes or reverts IKEv1/IKEv2 peer settings

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

## Syntax

```
no [authentication|ip|localid|remoteid|use <IKEv1/IKEv2-POLICY-NAME>]
```

## Parameters

no <PARAMETERS>

|                              |                                                                             |
|------------------------------|-----------------------------------------------------------------------------|
| <b>no &lt;PARAMETERS&gt;</b> | Removes or reverts IKEv1/IKEv2 peer settings based on the parameters passed |
|------------------------------|-----------------------------------------------------------------------------|

## Example

The following example shows the Crypto IKEV1 peer1 settings before the 'no' commands are executed:

```
nx9500-6C8809(config-profile-default-rfs4000-ikev1-peer-peer1)#show context
crypto ikev1 peer peer1
 ip address 172.16.10.12
 remoteid dn SanJose
 localid email bob@examplecompany.com
 use ikev1-policy test-ikev1policy
nx9500-6C8809(config-profile-default-rfs4000-ikev1-peer-peer1)#

nx9500-6C8809(config-profile-default-rfs4000-ikev1-peer-peer1)#no localid
nx9500-6C8809(config-profile-default-rfs4000-ikev1-peer-peer1)#no remoteid
```

The following example shows the Crypto IKEV1 peer1 settings after the 'no' commands are executed:

```
nx9500-6C8809(config-profile-default-rfs4000-ikev1-peer-peer1)#show context
crypto ikev1 peer peer1
 ip address 172.16.10.12
 use ikev1-policy test-ikev1policy
nx9500-6C8809(config-profile-default-rfs4000-ikev1-peer-peer1)#
```

The following example shows the Crypto IKEV2 peer1 settings before the 'no' commands are executed:

```
nx9500-6C8809(config-profile-default-rfs4000-ikev2-peer-peer1)#show context
crypto ikev2 peer peer1
 remoteid address 157.235.209.63
 use ikev2-policy test
nx9500-6C8809(config-profile-default-rfs4000-ikev2-peer-peer1)#
```

The following example shows the Crypto IKEV2 peer1 settings after the 'no' commands are executed:

```
nx9500-6C8809(config-profile-default-rfs4000-ikev2-peer-peer1)#no use ikev2-policy

nx9500-6C8809(config-profile-default-rfs4000-ikev2-peer-peer1)#show context
crypto ikev2 peer peer1
 remoteid address 157.235.209.63
nx9500-6C8809(config-profile-default-rfs4000-ikev2-peer-peer1)#
```

## crypto-map-config-commands

[crypto](#) on page 931

This section explains crypto map configuration mode commands in detail.

A crypto map entry is a single policy that describes how certain traffic is secured. There are two types of crypto map entries: ipsec-manual and ipsec-ike. Each entry is given an index (used to sort the ordered list).

IPSec VPN provides a secure tunnel between two networked peers. Administrators can define which packets are sent within the tunnel, and how they're protected. When a tunneled peer sees a sensitive packet, it creates a secure tunnel and sends the packet through the tunnel to its remote peer destination.

Tunnels are sets of SA between two peers. SAs define the protocols and algorithms applied to sensitive packets and specify the keying mechanisms used by tunneled peers. SAs are unidirectional and exist in both the inbound and outbound direction. SAs are established per the rules and conditions of defined security protocols (AH or ESP).

IKE is a key management protocol standard used in conjunction with IPSec. IKE enhances IPSec by providing additional features, flexibility, and configuration simplicity for the IPSec standard. IKE

automatically negotiates IPsec SAs, and enables secure communications without time consuming manual pre-configuration.

Use crypto maps to configure IPsec VPN SAs. Crypto maps combine the elements comprising IPsec SAs. Crypto maps also include transform sets. A transform set is a combination of security protocols, algorithms and other settings applied to IPsec protected traffic. One crypto map is utilized for each IPsec peer, however for remote VPN deployments one crypto map is used for all the remote IPsec peers.

Use the (config) instance to enter the crypto map configuration mode. To navigate to the crypto-map configuration instance, use the following commands:

In the device-config mode:

```
<DEVICE>(config-device-<DEVICE-MAC>)#crypto map <CRYPTO-MAP-TAG> <1-1000> [ipsec-isakmp {dynamic}|ipsec-manual]
```

In the profile-config mode:

```
<DEVICE>(config-profile-<PROFILE-NAME>)#crypto map <CRYPTO-MAP-TAG> <1-1000> [ipsec-isakmp {dynamic}|ipsec-manual]
```

There are three different configurations defined for each listed crypto map: site-to-site manual (ipsec-manual), site-to-site-auto tunnel (ipsec-isakmp), and remote VPN client (ipsec-isakmp dynamic). With site-to-site deployments, an IPsec tunnel is deployed between two gateways, each at the edge of two different remote networks. With remote VPN, an access point located at remote branch defines a tunnel with a security gateway. This facilitates the end points in the branch office to communicate with the destination endpoints (behind the security gateway) in a secure manner.

Each crypto map entry is given an index (used to sort the ordered list).

```
nx9500-6C8809(config-profile-default-rfs4000)#crypto map map1 1 ipsec-manual
nx9500-6C8809(config-profile-default-rfs4000-cryptomap-map1#1)#?
```

Manual Crypto Map Configuration commands:

|                      |                                                                                                    |
|----------------------|----------------------------------------------------------------------------------------------------|
| local-endpoint-ip    | Use this IP as local tunnel endpoint address, instead of the interface IP (Advanced Configuration) |
| mode                 | Set the tunnel mode                                                                                |
| no                   | Negate a command or set its defaults                                                               |
| peer                 | Set peer                                                                                           |
| security-association | Set security association parameters                                                                |
| session-key          | Set security session key parameters                                                                |
| use                  | Set setting to use                                                                                 |
| clearscr             | Clears the display screen                                                                          |
| commit               | Commit all changes made in this session                                                            |
| do                   | Run commands from Exec mode                                                                        |
| end                  | End current mode and change to EXEC mode                                                           |
| exit                 | End current mode and down to previous mode                                                         |
| help                 | Description of the interactive help system                                                         |
| revert               | Revert changes                                                                                     |
| service              | Service Commands                                                                                   |
| show                 | Show running system information                                                                    |
| write                | Write running configuration to memory or terminal                                                  |

```
nx9500-6C8809(config-profile-default-rfs4000-cryptomap-map1#1)#
```

The following table summarizes crypto map configuration mode commands:



| Command                                                                           | Description                                              |
|-----------------------------------------------------------------------------------|----------------------------------------------------------|
| <a href="#">crypto-map auto-vpn-tunnel/remote-vpn-client instance</a> on page 957 | Configures an auto site-to-site VPN or remote VPN client |
| <a href="#">crypto-map-ipsec-manual-instance</a> on page 968                      | Configures a manual site-to-site VPN                     |

crypto-map auto-vpn-tunnel/remote-vpn-client instance

[crypto-map-config-commands](#) on page 955

To navigate to the auto site-to-site VPN tunnel configuration instance, use the following command:

In the device-config mode:

```
<DEVICE>(config-device-<DEVICE-MAC>)#crypto map <CRYPTO-MAP-TAG> <1-1000> ipsec-isakmp
```

In the profile-config mode:

```
<DEVICE>(config-profile-<PROFILE-NAME>)#crypto map <CRYPTO-MAP-TAG> <1-1000> ipsec-isakmp
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58)#crypto map test 1 ipsec-isakmp
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#?
```

Site to Site Crypto Map Configuration commands:

```
ip Internet Protocol config commands
local-endpoint-ip Use this IP as local tunnel endpoint address, instead
of the interface IP (Advanced Configuration)
no Negate a command or set its defaults
peer Add a remote peer
pfs Specify Perfect Forward Secrecy
security-association Security association parameters
transform-set Specify IPSec transform to use
use Set setting to use

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#
```

To navigate to the remote VPN client configuration instance, use the following command:

In the device-config mode:

```
<DEVICE>(config-device-<DEVICE-MAC>)#crypto map <CRYPTO-MAP-TAG> <1-1000> ipsec-isakmp
{dynamic}
```

In the profile-config mode:

```
<DEVICE>(config-profile-<PROFILE-NAME>)#crypto map <CRYPTO-MAP-TAG> <1-1000> ipsec-isakmp
{dynamic}
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58)#crypto map test 2 ipsec-isakmp dynamic
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#?
```

Dynamic Crypto Map Configuration commands:

```
local-endpoint-ip Use this IP as local tunnel endpoint address, instead
```

```

of the interface IP (Advanced Configuration)
modeconfig Set the mode config method
no Negate a command or set its defaults
peer Add a remote peer
pfs Specify Perfect Forward Secrecy
remote-type Set the remote VPN client type
security-association Security association parameters
transform-set Specify IPSec transform to use
use Set setting to use

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```

The following table lists the IPSec-Auto-VPN/Remote-VPN tunnel configuration commands:

| Command                                          | Description                                                                                                                                                            |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">ip</a> on page 958                   | Enables this setting to utilize IP/Port NAT on the VPN tunnel. This command is applicable only to the site-to-site VPN tunnel.                                         |
| <a href="#">local-endpoint-ip</a> on page 959    | Uses the configured IP as local tunnel endpoint address, instead of the interface IP. This command is applicable to the site-to-site VPN tunnel and remote VPN client. |
| <a href="#">modeconfig</a> on page 960           | Configures the mode config method (pull or push) associated with the remote VPN client. This command is applicable only to the remote VPN client.                      |
| <a href="#">peer</a> on page 960                 | Configures the IKEv1 or IKEv2 peer for the VPN tunnel. This command is applicable to the site-to-site VPN tunnel and remote VPN client.                                |
| <a href="#">pfs</a> on page 961                  | Configures the Perfect Forward Secrecy (PFS) for the VPN tunnel. This command is applicable to the site-to-site VPN tunnel and remote VPN client.                      |
| <a href="#">remote-type</a> on page 962          | Configures the remote VPN client type as either None or XAuth. This command is applicable only to the remote VPN client.                                               |
| <a href="#">security-association</a> on page 963 | Defines this automatic VPN tunnel's IPSec SA settings. This command is applicable to the site-to-site VPN tunnel and remote VPN client.                                |
| <a href="#">transform-set</a> on page 964        | Applies a transform set (encryption and hash algorithms) to the VPN tunnel. This command is applicable to the site-to-site VPN tunnel and remote VPN client.           |
| <a href="#">use</a> on page 965                  | Applies an existing and configured IP access list to the VPN tunnel. This command is applicable to the site-to-site VPN tunnel and remote VPN client.                  |
| <a href="#">no</a> on page 966                   | Removes or reverts site-to-site VPN tunnel or remote VPN client settings                                                                                               |

[ip](#)

[crypto-map auto-vpn-tunnel/remote-vpn-client instance](#) on page 957

Enables this setting to utilize IP/Port NAT on this auto site-to-site VPN tunnel. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ip nat crypto
```

Parameters

```
ip nat crypto
```

|                      |                                                                                                                  |
|----------------------|------------------------------------------------------------------------------------------------------------------|
| <b>ip nat crypto</b> | Enables this setting to utilize IP/Port NAT on the site-to-site VPN tunnel. This setting is disabled by default. |
|----------------------|------------------------------------------------------------------------------------------------------------------|

Example

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#ip nat crypto
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
crypto map test 1 ipsec-isakmp
ip nat crypto
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#
```

local-endpoint-ip

[crypto-map auto-vpn-tunnel/remote-vpn-client instance](#) on page 957

Uses the configured IP as local tunnel endpoint address, instead of the interface IP

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
local-endpoint-ip <IP>
```

Parameters

```
local-endpoint-ip <IP>
```

|                                     |                                                                                                                                                                                                                                                          |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>local-endpoint-ip &lt;IP&gt;</b> | Configures the local VPN tunnel's (site-to-site VPN tunnel or remote VPN client) endpoint IP address <ul style="list-style-type: none"><li>• &lt;IP&gt; - Specify the IP address. The specified IP address must be available on the interface.</li></ul> |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Example

Site-to-site VPN tunnel:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#local-endpoint-ip
192.168.13.10
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
crypto map test 1 ipsec-isakmp
local-endpoint-ip 192.168.13.10
```

```

ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#

Remote VPN client:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#local-endpoint-ip
157.235.204.62

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
crypto map test 2 ipsec-isakmp dynamic
local-endpoint-ip 157.235.204.62
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
modeconfig

```

[crypto-map auto-vpn-tunnel/remote-vpn-client instance](#) on page 957

Configures the mode config method (pull or push) associated with the remote VPN client

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
modeconfig [pull|push]
```

Parameters

```
modeconfig [pull|push]
```

|                                         |                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>modeconfig</b><br><b>[pull push]</b> | Configures the mode config method associated with a remote VPN client. The options are: pull and push.<br>The mode (pull or push) defines the method used to assign a virtual IP. This setting is relevant for IKEv1 only, since IKEv2 always uses the configuration payload in pull mode. The default setting is push. |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Example

```

Remote VPN client:

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#modeconfig pull

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
crypto map test 2 ipsec-isakmp dynamic
modeconfig pull
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)
peer

```

[crypto-map auto-vpn-tunnel/remote-vpn-client instance](#) on page 957

Configures the IKEv1 or IKEv2 peer for the auto site-to-site VPN tunnel or remote VPN client. The peer device can be specified either by its hostname or by its IP address. A maximum of three peers can be configured.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
peer <1-3> [ikev1|ikev2] <IKEv1/IKEv2-PEER-NAME>
```

#### Parameters

```
peer <1-3> [ikev1|ikev2] <IKEv1/IKEv2-PEER-NAME>
```

|                                      |                                                                                                                                       |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <b>peer &lt;1-3&gt;</b>              | Creates a new peer and configures the peer's priority level. Peer '1' is the primary peer, and peer '3' is redundant.                 |
| <b>ikev1 &lt;IKEv1-PEER-NAME&gt;</b> | Configures an IKEv1 peer <ul style="list-style-type: none"> <li>• &lt;IKEv1-PEER-NAME&gt; - Specify the IKEv1 peer's name.</li> </ul> |
| <b>ikev2&lt;IKEv2-PEER-NAME&gt;</b>  | Configures an IKEv2 peer <ul style="list-style-type: none"> <li>• &lt;IKEv2-PEER-NAME&gt; - Specify the IKEv2 peer's name.</li> </ul> |

#### Example

Site-to-site tunnel:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#peer 1 ikev2 ikev2Peer1
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
crypto map test 1 ipsec-isakmp
peer 1 ikev2 ikev2Peer1
local-endpoint-ip 192.168.13.10
ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#
```

Remote VPN client:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#peer 1 ikev1 Re
moteIKEv1Peer1

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
crypto map test 2 ipsec-isakmp dynamic
peer 1 ikev1 RemoteIKEv1Peer1
local-endpoint-ip 157.235.204.62
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```

pfs

[crypto-map auto-vpn-tunnel/remote-vpn-client instance](#) on page 957

Configures Perfect Forward Secrecy (PFS) for the auto site-to-site VPN tunnel or remote VPN client

PFS is the key-establishment protocol, used to secure VPN communications. If one encryption key is compromised, only data encrypted by that specific key is compromised. For PFS to exist, the key used to protect data transmissions must not be used to derive any additional keys. Options include 2, 5 and 14. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000

- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

**pfs** [14|2|5]

Parameters

**pfs** [14|2|5]

|                     |                                                                                                                                                                                                                                 |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>pfs</b> [14 2 5] | <p>Configures PFS</p> <ul style="list-style-type: none"> <li>• 14 – Configures D-H Group14 (2048-bit modp)</li> <li>• 2 – Configures D-H Group2 (1024-bit modp)</li> <li>• 5 – Configures D-H Group5 (1536-bit modp)</li> </ul> |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Example

Site-to-site VPN tunnel:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#pfs 5

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
crypto map test 1 ipsec-isakmp
 peer 1 ikev2 ikev2Peer1
 local-endpoint-ip 192.168.13.10
 pfs 5
 ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#
```

Remote VPN client:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#pfs 14

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
crypto map test 2 ipsec-isakmp dynamic
 peer 1 ikev1 RemoteIKEv1Peer1
 local-endpoint-ip 157.235.204.62
 pfs 14
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```

remote-type

[crypto-map auto-vpn-tunnel/remote-vpn-client instance](#) on page 957

Configures the remote VPN client type as either None or XAuth

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

**remote-type** [none|xauth]

Parameters

**remote-type** [none|xauth]

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>remote-type</b><br><b>[none   xauth]</b> | <p>Specify the remote VPN's client type</p> <ul style="list-style-type: none"> <li>• none – Configures remote VPN client with No XAUTH</li> <li>• xauth – Configures remote VPN client as using XAUTH (applicable only for IKEv1). This is the default setting.</li> </ul> <p>XAuth (extended authentication) provides additional authentication validation by permitting an edge device to request extended authentication information from an IPSec host. This forces the host to respond with additional authentication credentials. The edge device respond with a failed or passed message.</p> |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Example

Remote VPN client:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#remote-type none

rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
crypto map test 2 ipsec-isakmp dynamic
peer 1 ikev1 RemoteIKEv1Peer1
local-endpoint-ip 157.235.204.62
pfs 14
remote-type none
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```

security-association

[crypto-map auto-vpn-tunnel/remote-vpn-client instance](#) on page 957

Defines the IPSec SA's (created by this auto site-to-site VPN tunnel or remote VPN client) settings

Supported in the following platforms:

- Access Points – AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers – RFS4000
- Service Platforms – NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
security-association [inactivity-timeout | level | lifetime]
```

```
security-association [inactivity-timeout <120-86400> | level perhost]
security-association lifetime [kilobytes <500-2147483646> | seconds <120-86400>]
```

Parameters

```
security-association [inactivity-timeout <120-86400> | level perhost]
```

|                                                       |                                                                                                                                                                                                                                                                                       |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>inactivity-timeout</b><br><b>&lt;120-86400&gt;</b> | <p>Specifies an inactivity period, in seconds, for this IPSec VPN SA. Once the set value is exceeded, the association is timed out.</p> <ul style="list-style-type: none"> <li>• &lt;120-86400&gt; – Specify a value from 120 - 86400 seconds. The default is 900 seconds.</li> </ul> |
| <b>level perhost</b>                                  | <p>Specifies the granularity level for this IPSec VPN SA</p> <ul style="list-style-type: none"> <li>• perhost – Sets the IPSec VPN SA's granularity to the host level</li> </ul>                                                                                                      |

```
security-association lifetime [kilobytes <500-2147483646> | seconds <120-86400>]
```



|                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>lifetime</b><br><b>[kilobytes</b><br><b>&lt;500-2147483646</b><br><b>&gt;  seconds</b><br><b>&lt;120-86400&gt;]</b> | Defines the IPsec SA's lifetime (in kilobytes and/or seconds). Values can be entered in both kilobytes and seconds. Which ever limit is reached first, ends the security association. <ul style="list-style-type: none"> <li>• kilobytes &lt;500-2147483646&gt; – Defines volume based key duration. Specify a value from 500 - 2147483646 kilobytes. Select this option to define a connection volume lifetime (in kilobytes) for the duration of the IPsec VPN SA. Once the set volume is exceeded, the association is timed out. This option is disabled by default.</li> <li>• seconds &lt;120-86400&gt; – Defines time based key duration. Specify the time frame from 120 - 86400 seconds. Select this option to define a lifetime (in seconds) for the duration of the IPsec VPN SA. Once the set value is exceeded, the association is timed out. This option is disabled by default.</li> </ul> |
|------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Example

Site-to-site tunnel:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#security-association
inactivity-timeout 200
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#security-association
level perhost
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#security-association
lifetime kilobytes 250000
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
crypto map test 1 ipsec-isakmp
 security-association level perhost
 peer 1 ikev2 ikev2Peer1
 local-endpoint-ip 192.168.13.10
 pfs 5
 security-association lifetime kilobytes 250000
 security-association inactivity-timeout 200
 ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#
```

Remote VPN client:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#security-association
lifetime seconds 10000
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
crypto map test 2 ipsec-isakmp dynamic
peer 1 ikev1 RemoteIKEv1Peer1
local-endpoint-ip 157.235.204.62
pfs 14
security-association lifetime seconds 10000
remote-type none
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```

transform-set

[crypto-map auto-vpn-tunnel/remote-vpn-client instance](#) on page 957

Applies a transform set (encryption and hash algorithms) to site-to-site VPN tunnel or remote VPN client. This command allows you to provide customized data protection for each crypto map can be customized with its own data protection and peer authentication schemes.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533



- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
transform-set <TRANSFORM-SET-TAG> {<TRANSFORM-SET-TAG>}
```

#### Parameters

```
transform-set <TRANSFORM-SET-TAG> {<TRANSFORM-SET-TAG>}
```

|                                  |                                                                                                                                                                                                                                                                   |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>transform-set</b>             | Applies a transform set. The transform set should be existing and configured.                                                                                                                                                                                     |
| <b>&lt;TRANSFORM-SET-TAG&gt;</b> | <ul style="list-style-type: none"> <li>• &lt;TRANSFORM-SET-TAG&gt; - Specify the transform set's name.</li> <li>• &lt;TRANSFORM-SET-TAG&gt; - Optional. Specify a second transform set. You can provide multiple, space-separated, transform set tags.</li> </ul> |

#### Example

Site-to-site VPN tunnel:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#transform-set AutoVPN
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
crypto map test 1 ipsec-isakmp
 security-association level perhost
 peer 1 ikev2 ikev2Peer1
 local-endpoint-ip 192.168.13.10
 pfs 5
 security-association lifetime kilobytes 250000
 security-association inactivity-timeout 200
 transform-set AutoVPN
 ip nat crypto
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#
```

Remote VPN client:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#transform-set RemoteVPN
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
crypto map test 2 ipsec-isakmp dynamic
 peer 1 ikev1 RemoteIKEv1Peer1
 local-endpoint-ip 157.235.204.62
 pfs 14
 security-association lifetime seconds 10000
 transform-set RemoteVPN
 remote-type none
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```

use

[crypto-map auto-vpn-tunnel/remote-vpn-client instance](#) on page 957

Applies an existing and configured IP access list to the auto site-to-site VPN tunnel or remote VPN client. Based on the IP access list's settings traffic is permitted or denied across the VPN tunnel.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000

- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
use ip-access-list <IP-ACCESS-LIST-NAME>
```

#### Parameters

```
use ip-access-list <IP-ACCESS-LIST-NAME>
```

**ip-access-list** Specify the IP access list name.  
**<IP-ACCESS-LIST-NAME>**

#### Example

Site-to-site VPN tunnel:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#use ip-access-list test
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
crypto map test 1 ipsec-isakmp
 use ip-access-list test
 security-association level perhost
 peer 1 ikev2 ikev2Peer1
 local-endpoint-ip 192.168.13.10
 pfs 5
 security-association lifetime kilobytes 250000
 security-association inactivity-timeout 200
 transform-set AutoVPN
 ip nat crypto
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#
```

Remote VPN client:

```
rrfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#use ip-access-list test1
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
' crypto map test 2 ipsec-isakmp dynamic
 use ip-access-list test1
 peer 1 ikev1 RemoteIKEv1Peer1
 local-endpoint-ip 157.235.204.62
 pfs 14
 security-association lifetime seconds 10000
 transform-set RemoteVPN
 remote-type none
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```

no

[crypto-map auto-vpn-tunnel/remote-vpn-client instance](#) on page 957

Removes or reverts the auto site-to-site VPN tunnel or remote VPN client settings

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
no [ip|local-endpoint-ip|modeconfig|peer|pfs|remote-type|security-association| transform-set|use]
```

Parameters

no <PARAMETERS>

|                           |                                                                                      |
|---------------------------|--------------------------------------------------------------------------------------|
| <b>no</b>                 | Removes or resets this auto site-to-site/remote VPN settings based on the parameters |
| <b>&lt;PARAMETERS&gt;</b> | passed                                                                               |

Example

The following example shows the IPSec site-to-site VPN tunnel 'test' settings before the 'no' commands are executed:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
crypto map test 1 ipsec-isakmp
 use ip-access-list test
 security-association level perhost
 peer 1 ikev2 ikev2Peer1
 local-endpoint-ip 192.168.13.10
 pfs 5
 security-association lifetime kilobytes 250000
 security-association inactivity-timeout 200
 transform-set AutVPN
 ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#no use ip-access-list
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#no security-association
level perhost
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#no ip nat crypto
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#no pfs
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#no local-endpoint-ip
```

The following example shows the IPSec site-to-site VPN tunnel 'test' settings after the 'no' commands are executed:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#show context
crypto map test 1 ipsec-isakmp
 peer 1 ikev2 ikev2Peer1
 security-association lifetime kilobytes 250000
 security-association inactivity-timeout 200
 transform-set AutoVPN
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#1)#
```

The following example shows the IPSec remote VPN client 'test' settings before the 'no' commands are executed:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
crypto map test 2 ipsec-isakmp dynamic
 use ip-access-list test2
 peer 1 ikev1 RemoteIKEv1Peer1
 local-endpoint-ip 157.235.204.62
 pfs 14
 security-association lifetime seconds 10000
 transform-set RemoteVPN
 remote-type none
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#no use ip-access-list
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#no peer 1
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#no transform-set
```

The following example shows the IPsec remote VPN client 'test' settings after the 'no' commands are executed:

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#show context
crypto map test 2 ipsec-isakmp dynamic
 local-endpoint-ip 157.235.204.62
 pfs 14
 security-association lifetime seconds 10000
 remote-type none
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#2)#
crypto-map-ipsec-manual-instance
```

[crypto-map-config-commands](#) on page 955

To navigate to the automatic IPsec manual VPN tunnel configuration instance, use the following command:

In the device-config mode:

```
<DEVICE>(config-device-<DEVICE-MAC>)#crypto map <CRYPTO-MAP-TAG> <1-1000> ipsec-manual
```

In the profile-config mode:

```
<DEVICE>(config-profile-<PROFILE-NAME>)#crypto map <CRYPTO-MAP-TAG> <1-1000> ipsec-manual
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58)#crypto map test 3 ipsec-manual
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#3)#?
```

Manual Crypto Map Configuration commands:

|                                   |                                                                                                    |
|-----------------------------------|----------------------------------------------------------------------------------------------------|
| <code>local-endpoint-ip</code>    | Use this IP as local tunnel endpoint address, instead of the interface IP (Advanced Configuration) |
| <code>mode</code>                 | Set the tunnel mode                                                                                |
| <code>no</code>                   | Negate a command or set its defaults                                                               |
| <code>peer</code>                 | Set peer                                                                                           |
| <code>security-association</code> | Set security association parameters                                                                |
| <code>session-key</code>          | Set security session key parameters                                                                |
| <code>use</code>                  | Set setting to use                                                                                 |
| <code>clearscr</code>             | Clears the display screen                                                                          |
| <code>commit</code>               | Commit all changes made in this session                                                            |
| <code>do</code>                   | Run commands from Exec mode                                                                        |
| <code>end</code>                  | End current mode and change to EXEC mode                                                           |
| <code>exit</code>                 | End current mode and down to previous mode                                                         |
| <code>help</code>                 | Description of the interactive help system                                                         |
| <code>revert</code>               | Revert changes                                                                                     |
| <code>service</code>              | Service Commands                                                                                   |
| <code>show</code>                 | Show running system information                                                                    |
| <code>write</code>                | Write running configuration to memory or terminal                                                  |

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-cryptomap-test#3)#
```

The following table summarizes IPsec manual VPN tunnel configuration mode commands:

| Command                                       | Description                                                                                                   |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| <code>local-endpoint-ip</code> on page 969    | Uses the configured IP as local tunnel endpoint address, instead of the interface IP (Advanced Configuration) |
| <code>mode</code> on page 969                 | Sets the tunnel mode                                                                                          |
| <code>peer</code> on page 970                 | Sets the peer device's IP address                                                                             |
| <code>security-association</code> on page 970 | Defines the lifetime (in kilobytes and/or seconds) of IPsec SAs created by a crypto map                       |

| Command                                 | Description                                                 |
|-----------------------------------------|-------------------------------------------------------------|
| <a href="#">session-key</a> on page 971 | Defines encryption and authentication keys for a crypto map |
| <a href="#">use</a> on page 973         | Uses the configured IP access list                          |
| <a href="#">no</a> on page 973          | Removes or reverts crypto map IPsec manual settings         |

## local-endpoint-ip

[crypto-map-ipsec-manual-instance](#) on page 968

Uses the configured IP as local tunnel endpoint address, instead of the interface IP (Advanced Configuration)

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

**local-endpoint-ip** <IP>

Parameters

**local-endpoint-ip** <IP>

|                               |                                                                                                                                                                                                                        |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>local-endpoint-ip</b> <IP> | <p>Uses the configured IP as local tunnel's endpoint address</p> <ul style="list-style-type: none"> <li>• &lt;IP&gt; - Specify the IP address. The specified IP address must be available on the interface.</li> </ul> |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Example

```
nx9500-6C8809(config-profile-default-rfs4000-cryptomap-map1#1)#local-endpoint-ip 172.16.10.3
```

mode

[crypto-map-ipsec-manual-instance](#) on page 968

Sets the crypto map tunnel mode

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

**mode** [transport|tunnel]

Parameters

**mode** [transport|tunnel]

|                                  |                                                                                                                                                                                                   |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mode [transport   tunnel]</b> | Sets the mode of the tunnel for this crypto map <ul style="list-style-type: none"><li>• transport – Initiates transport mode</li><li>• tunnel – Initiates tunnel mode (default setting)</li></ul> |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Example

```
nx9500-6C8809(config-profile-default-rfs4000-cryptomap-map1#1)#mode transport
```

```
nx9500-6C8809(config-profile-default-rfs4000-cryptomap-map1#1)#show context
crypto map map1 1 ipsec-manual
mode transport
```

```
nx9500-6C8809(config-profile-default-rfs4000-cryptomap-map1#1)#
```

peer

[crypto-map-ipsec-manual-instance](#) on page 968

Sets the peer device's IP address. This can be set for multiple remote peers. The remote peer can be an IP address.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
peer <IP>
```

#### Parameters

```
peer <IP>
```

|                        |                                                                                        |
|------------------------|----------------------------------------------------------------------------------------|
| <b>peer &lt;IP&gt;</b> | Enter the peer device's IP address. If not configured, it implies respond to any peer. |
|------------------------|----------------------------------------------------------------------------------------|

#### Example

```
nx9500-6C8809(config-profile-default-rfs4000-cryptomap-map1#1)#peer 172.16.10.12
```

```
nx9500-6C8809(config-profile-default-rfs4000-cryptomap-map1#1)#show context
crypto map map1 1 ipsec-manual
peer 172.16.10.12
```

```
nx9500-6C8809(config-profile-default-rfs4000-cryptomap-map1#1)#
```

security-association

[crypto-map-ipsec-manual-instance](#) on page 968

Defines the lifetime (in kilobytes and/or seconds) of IPSec SAs created by this crypto map

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
security-association lifetime [kilobytes <500-2147483646>|seconds
<120-86400>]
```

#### Parameters

```
security-association lifetime [kilobytes <500-2147483646>|seconds <120-86400>]
```

|                           |                                                                                                                        |
|---------------------------|------------------------------------------------------------------------------------------------------------------------|
| <b>lifetime</b>           | Values can be entered in both kilobytes and seconds. Which ever limit is reached first, ends the security association. |
| <b>[kilobytes</b>         |                                                                                                                        |
| <b>&lt;500-2147483646</b> | • kilobytes <500-2147483646> - Defines volume based key duration. Specify a value                                      |
| <b>&gt;  seconds</b>      | from 500 - 2147483646 bytes.                                                                                           |
| <b>&lt;120-86400&gt;]</b> | • seconds <120-86400> - Defines time based key duration. Specify the time frame                                        |
|                           | from 120 - 86400 seconds.                                                                                              |



#### Note

This command is not applicable to the ipsec-manual crypto map.

#### Example

```
nx9500-6C8809(config-profile-default-rfs4000-cryptomap-map2#2)#security-association
lifetime seconds 123
```

```
nx9500-6C8809(config-profile-default-rfs4000-cryptomap-map2#2)#show context
Command not applicable to this crypto map
```

```
nx9500-6C8809(config-profile-default-rfs4000-cryptomap-map2#2)#
```

session-key

[crypto-map-ipsec-manual-instance](#) on page 968

Defines encryption and authentication keys for this crypto map

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
session-key [inbound|outbound] [ah|esp] <256-4294967295>
```

```
session-key [inbound|outbound] ah <256-4294967295> [0|2|authenticator
[md5|sha]] <WORD>
```

```
session-key [inbound|outbound] esp <256-4294967295> [0|2|cipher [3des|
aes|aes-192| aes-256|des|esp-null]] <WORD> authenticator [md5|sha] <WORD>
```

#### Parameters

```
session-key [inbound|outbound] ah <256-4294967295> [0|2|authenticator [md5|sha]] <WORD>
```

|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>session-key</b><br>[ inbound  <br>outbound ]         | Defines the manual inbound and outbound security association key parameters                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>ah</b><br><256-4294967295><br>5>                     | Configures authentication header (AH) as the security protocol for the security session <ul style="list-style-type: none"> <li>&lt;256-4294967295&gt; - Sets the SPI for the security association from 256 - 4294967295</li> </ul> <p>The SPI (in combination with the destination IP address and security protocol) identifies the security association.</p>                                                                                                                                                      |
| [ 0   2  <br>authenticator<br>[ md5   sha ]<br><WORD> ] | Specifies the key type <ul style="list-style-type: none"> <li>0 - Sets a clear text key</li> <li>2 - Sets an encrypted key</li> <li>authenticator - Sets AH authenticator details <ul style="list-style-type: none"> <li>md5 &lt;WORD&gt; - AH with MD5 authentication</li> <li>sha &lt;WORD&gt; - AH with SHA authentication</li> </ul> </li> </ul> <p>&lt;WORD&gt; - Sets security association key value. The following key lengths (in hex characters) are required (w/o leading 0x).AH-MD5: 32, AH-SHA: 40</p> |

```
session-key [inbound|outbound] esp <256-4294967295> [0 | 2 | cipher [3des | aes | aes-192 | aes-256 |
des | esp-null]] <WORD> authenticator [md5 | sha] <WORD>
```

|                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>session-key</b><br>[ inbound  <br>outbound ]                                    | Defines the manual inbound and outbound security association key parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>esp</b><br><256-4294967295><br>5>                                               | Configures Encapsulating Security Payloads (ESP) as the security protocol for the security session. This is the default setting. <ul style="list-style-type: none"> <li>&lt;256-4294967295&gt; - Sets the SPI for the security association from 256 - 4294967295</li> </ul> <p>The SPI (in combination with the destination IP address and security protocol) identifies the security association.</p>                                                                                                                                                                                                                                                                                                                                                                                                         |
| [ 0   2   cipher<br>[ 3des   aes  <br>aes-192  <br>aes-256   des  <br>esp-null ] ] | <ul style="list-style-type: none"> <li>0 - Sets a clear text key</li> <li>2 - Sets an encrypted key</li> <li>cipher - Sets encryption/decryption key details <ul style="list-style-type: none"> <li>3des - ESP with 3DES encryption</li> <li>aes - ESP with AES encryption</li> <li>aes-192 - ESP with AES-192 encryption</li> <li>aes-256 - ESP with AES-256 encryption</li> <li>des - ESP with DES encryption</li> <li>esp-null - ESP with no encryption</li> </ul> </li> </ul> <p>authenticator - Specify ESP authenticator details<br/>md5 &lt;WORD&gt; - ESP with MD5 authentication<br/>sha &lt;WORD&gt; - ESP with SHA authentication</p> <p>&lt;WORD&gt; - Sets security association key value. The following key lengths (in hex characters) are required (w/o leading 0x).AH-MD5: 32, AH-SHA: 40</p> |

#### Example

```
nx9500-6C8809(config-profile-default-rfs4000-cryptomap-map1#1)#session-key inbound esp 273
cipher esp-null authenticator sha 58768979
```



```
nx9500-6C8809(config-profile-default-rfs4000-cryptomap-map1#1)#show context
crypto map map1 1 ipsec-manual
peer 172.16.10.2
mode transport
session-key inbound esp 273 0 cipher esp-null authenticator sha 58768979
nx9500-6C8809(config-profile-default-rfs4000-cryptomap-map1#1)#
```

use

[crypto-map-ipsec-manual-instance](#) on page 968

Associates an existing IP access list with this crypto map. The ACL protects the VPN traffic.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
use ip-access-list <IP-ACCESS-LIST-NAME>
```

Parameters

```
use ip-access-list <IP-ACCESS-LIST-NAME>
```

|                                                                                                      |
|------------------------------------------------------------------------------------------------------|
| <p><b>ip-access-list</b> Specify the IP access list name.<br/><b>&lt;IP-ACCESS-LIST-NAME&gt;</b></p> |
|------------------------------------------------------------------------------------------------------|

Example

```
nx9500-6C8809(config-profile-default-rfs4000-cryptomap-map1#1)#use ip-access-list test

nx9500-6C8809(config-profile-default-rfs4000-cryptomap-map1#1)#show context
crypto map map1 1 ipsec-manual
use ip-access-list test
peer 172.16.10.12
mode transport
session-key inbound esp 273 0 cipher esp-null authenticator sha 5876897
nx9500-6C8809(config-profile-default-rfs4000-cryptomap-map1#1)#
```

no

[crypto-map-ipsec-manual-instance](#) on page 968

Removes or resets this crypto map's settings

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [local-endpoint-ip|mode|peer|security-association|session-key|use]
```

## Parameters

no <PARAMETERS>

|                                        |                                                                           |
|----------------------------------------|---------------------------------------------------------------------------|
| <b>no</b><br><b>&lt;PARAMETERS&gt;</b> | Removes or resets this crypto map settings based on the parameters passed |
|----------------------------------------|---------------------------------------------------------------------------|

## Example

```
nx9500-6C8809(config-profile-default-rfs4000-cryptomap-map1#)#show context
crypto map map1 1 ipsec-manual
 use ip-access-list test
 peer 172.16.10.12
 mode transport
 session-key inbound esp 273 0 cipher esp-null authenticator sha 5876897
nx9500-6C8809(config-profile-default-rfs4000-cryptomap-map1#)#
```

```
nx9500-6C8809(config-profile-default-rfs4000-cryptomap-map1#)#no use ip-access-list
nx9500-6C8809(config-profile-default-rfs4000-cryptomap-map1#)#no peer
nx9500-6C8809(config-profile-default-rfs4000-cryptomap-map1#)#no mode
```

```
nx9500-6C8809(config-profile-default-rfs4000-cryptomap-map1#)#show context
crypto map map1 1 ipsec-manual
 session-key inbound esp 273 0 cipher esp-null authenticator sha 58768979
nx9500-6C8809(config-profile-default-rfs4000-cryptomap-map1#)#
```

## crypto-remote-vpn-client commands

[crypto](#) on page 931

This section documents the IKEV2 remote VPN client configuration settings. Use this command to define the server resources used to secure (authenticate) a remote VPN connection with a target peer.

Use the profile-config instance to configure remote VPN client settings. To navigate to the remote-vpn-client configuration instance, use the following commands:

```
<DEVICE>(config)#profile <DEVICE-TYPE> <PROFILE-NAME>
<DEVICE>(config-profile-<PROFILE-NAME>)#crypto remote-vpn-client
<DEVICE>(config-profile-<PROFILE-NAME>-crypto-ikev2-remote-vpn-client)#
```

### Note

To configure remote VPN client settings on a device, on the device's configuration mode, use the `crypto > remote-vpn-client` command. For example: `rfs4000-229D58(config-device-00-23-68-22-9D-58)#crypto remote-vpn-client`

The following configuration enables a access point to adopt to a controller over the remote VPN link:

- On a profile: `rfs4000-229D58(config-profile-testRFS4000)#controller host <HOST-IP> remote-vpn-client`
- On a device: `rfs4000-229D58(config-00-23-68-22-9D-58)#controller host <HOST-IP> remote-vpn-client`  
`rfs4000-229D58(config)#profile rfs4000 testRFS4000`  
`rfs4000-229D58(config-profile-testRFS4000)#`



```
rfs4000-229D58(config-profile-testRFS4000)#crypto remote-vpn-client
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#?
Crypto IKEV2 Remote Vpn Client Config commands:
dhcp-peer Configure parameters for peers received via DHCP option
no Negate a command or set its defaults
peer Add a remote peer
shutdown Disable remote vpn client
transform-set Specify IPSec transform to use

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#
```

The following table summarizes `crypto remote VPN client` configuration mode commands:

| Command                                | Description                                                            |
|----------------------------------------|------------------------------------------------------------------------|
| <code>dhcp-peer</code> on page 976     | Configures DHCP peer's local ID and authentication settings            |
| <code>peer</code> on page 976          | Adds a remote IKEv2 peer                                               |
| <code>shutdown</code> on page 977      | Disables the remote VPN client                                         |
| <code>transform-set</code> on page 978 | Associates an existing IPSec transform set with this remote VPN client |
| <code>no</code> on page 978            | Removes the remote VPN client settings                                 |

## dhcp-peer

[crypto-remote-vpn-client commands](#) on page 974

Configures DHCP peer's local ID and authentication settings

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
dhcp-peer [authentication|localid]
```

```
dhcp-peer authentication [psk [0 <WORD>|2 <WORD>|<WORD>]|rsa]
```

```
dhcp-peer localid [autogen-uniqueid <WORD>|string <WORD>]
```

Parameters

```
dhcp-peer authentication [psk [0 <WORD>|2 <WORD>|<WORD>]|rsa]
```

|                                                                                        |                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>dhcp-peer authentication [psk [0 &lt;WORD&gt; 2 &lt;WORD&gt; &lt;WORD&gt;] rsa]</b> | Configures the DHCP peer's authentication type as PSK <ul style="list-style-type: none"><li>• 0 &lt;WORD&gt; - Configures a clear text authentication key</li><li>• 2 &lt;WORD&gt; - Configures an encrypted authentication key</li><li>• &lt;WORD&gt; - Provide a 8 - 21 character shared key password for DHCP peer authentication</li></ul> |
| <b>dhcp-peer authentication rsa</b>                                                    | Configures the DHCP peer's authentication type as RSA. This is the default setting.                                                                                                                                                                                                                                                            |

```
dhcp-peer localid [autogen-uniqueid <WORD>|string <WORD>]
```

|                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>dhcp-peer localid [autogen-uniqueid &lt;WORD&gt; string &lt;WORD&gt;]</b> | Configures the DHCP peer's localid using one of the following options: <ul style="list-style-type: none"><li>• autogen-uniqueid - Generates a localid using the device's unique identity. The system prefixes the device's unique identity to the string provided here. The device's unique identity should be existing and configured. For more information on configuring a device's unique identity, see <a href="#">autogen-uniqueid</a> on page 883.<ul style="list-style-type: none"><li>• &lt;WORD&gt; - Provide the string.</li></ul></li><li>• string - Uses the value provided here as the DHCP peer's localid.<ul style="list-style-type: none"><li>• &lt;WORD&gt; - Provide the string.</li></ul></li></ul> |
|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Example

```
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#dhcp-peer authentication psk 0 @123testing
```

```
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#show context crypto remote-vpn-client
 dhcp-peer authentication psk 0 @123testing
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#
```

peer

[crypto-remote-vpn-client commands](#) on page 974

Configures IKEv2 peers and assigns them priorities for utilization with remote VPN client connections. A maximum of three (3) peers can be added to support redundancy.

IKEv2 uses an initial handshake in which VPN peers negotiate cryptographic algorithms, mutually authenticate, and establish a session key, creating an IKE-SA. Additionally, a first IPSec SA is established during the initial SA creation. All IKEv2 messages are request/response pairs. It is the responsibility of the side sending the request to retransmit if it does not receive a timely response.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
peer <1-3> ikev2 <IKEV2-PEER-NAME>
```

Parameters

```
peer <1-3> ikev2 <IKEV2-PEER-NAME>
```

|                                      |                                                                                                                                                                                                                                                    |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>peer &lt;1-3&gt;</b>              | Adds a IKEv2 peer. You can add maximum of three (3) peers to achieve redundancy. <ul style="list-style-type: none"><li>• &lt;1-3&gt; - Specify a priority level for the peer from 1 - 3 (1 = primary, 2 = secondary, and 3 = redundant).</li></ul> |
| <b>ikev2 &lt;IKEV2-PEER-NAME&gt;</b> | Specify the IKEv2 peer's name.<br><b>Note:</b> The peer should be existing and configured. To configure an IKEv2 peer use the <code>crypto &gt; ikev2 &gt; peer &gt; &lt;IKEV2-PEER-NAME&gt;</code> command.                                       |

Example

```
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#peer 1 ikev2 ikev2Peer1
```

```
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#peer 2 ikev2 ikev2Peer2
```

```
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#show context crypto remote-vpn-client peer 1 ikev2 ikev2Peer1 peer 2 ikev2 ikev2Peer2
```

```
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#
```

shutdown

[crypto-remote-vpn-client commands](#) on page 974

Disables remote-vpn-client on this profile or device. Remote VPN client feature is enabled by default.

To enable a disabled remote VPN client execute the `no > shutdown` command.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

**shutdown**

Parameters

None

Example

```
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#
shutdown
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#
```

transform-set

[crypto-remote-vpn-client commands](#) on page 974

Specifies the IPSec Transform set to use with this remote VPN client. A transform set is a combination of security protocols, algorithms, and other settings applied to IPSec protected client traffic.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

**transform-set** <IPSEC-XFORM-TAG> {<IPSEC-XFORM-TAG>}

Parameters

**transform-set** <IPSEC-XFORM-TAG> {<IPSEC-XFORM-TAG>}

|                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>transform-set</b><br/><b>&lt;IPSEC-XFORM-TAG&gt;</b> &lt;IPSEC-XFORM-TAG&gt;</p> | <p>Associates an IPSec Transform (should be existing and configured) set with this remote VPN client. You can optionally associate more than one transform set with this remote VPN client configuration. List the transform set tags separated by a space.</p> <p><b>Note:</b> To configure a transform-set, use the <code>crypto &gt; ipsec &gt; transform-set</code> command in the profile or device configuration mode.</p> |
|----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Example

```
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#transform-set
TransformSet1
```

```
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#show
context
crypto remote-vpn-client
peer 1 ikev2 ikev2Peer1
transform-set TransformSet1
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#
```

no

[crypto-remote-vpn-client commands](#) on page 974

Removes the remote VPN client settings

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [dhcp-peer|peer <1-3>|shutdown|transform-set]
```

```
no dhcp-peer [authentication|localid]
```

```
no peer <1-3>
```

```
no shutdown
```

```
no transform-set
```

Parameters

```
no <PARAMETERS>
```

|                                        |                                                                                  |
|----------------------------------------|----------------------------------------------------------------------------------|
| <b>no</b><br><b>&lt;PARAMETERS&gt;</b> | Removes or resets this remote VPN client settings based on the parameters passed |
|----------------------------------------|----------------------------------------------------------------------------------|

Example

```
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#show context
crypto remote-vpn-client
peer 1 ikev2 peer5
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#

rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#no peer 1

rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#show context
crypto remote-vpn-client
rfs4000-229D58(config-profile-testRFS4000-crypto-ikev2-remote-vpn-client)#
```

*database*

[Profile Config Commands](#) on page 862

Backs up captive-portal and/or NSight database to a specified location and file. When applied to devices, this profile will enable the back up of the specified database. This command also enables you to configure a low-disk-space threshold value.

These parameters can also be configured in the device configuration context of an NX95XX series service platform.

**Supported in the following platforms:**

- Service Platforms — NX9500, NX9510, NX9600, VX9000

**Syntax**

```
database [backup|low-disk-space-threshold]
```

```
database backup database [captive-portal|nsight] <URL>
```

```
database low-disk-space-threshold <10-50>
```

### Parameters

```
database backup database [captive-portal|nsight] <URL>
```

|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>database backup database [captive-portal nsight]</b> | <p>Backs up captive portal and/or NSight database to a specified location and file. Select the database to backup.</p> <ul style="list-style-type: none"><li>• database – Selects the database to backup</li><li>• captive-portal – Backs up captive portal database</li><li>• nsight – Backs up NSight database</li></ul> <p>After specifying the database type, configure the destination location and file name.</p> |
| <b>&lt;URL&gt;</b>                                      | <p>Configures the destination location. The database is backed up at the specified location. Specify the location URL in one of the following formats:</p> <pre>ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IP&gt;[:port]/path/file.tar.gz<br/>sftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IP&gt;[:port]/path/file.tar.gz<br/>tftp://&lt;hostname IP&gt;[:port]/path</pre>                                       |

```
database low-disk-space-threshold <10-50>
```

|                                                        |                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>database low-disk-space-threshold &lt;10-50&gt;</b> | <p>Configures the low disk space threshold for syslog warning. Once the threshold value configured here is reached a syslog warning is sent.</p> <ul style="list-style-type: none"><li>• &lt;10-50&gt; – Specify the threshold from 10 - 50. The default is 30.</li></ul> |
|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Example

```
nx9500-6C8809(config-profile-testNX9500)#database backup database nsight ftp://
anonymous:anonymous@192.168.13.10/backups/nsight/nsight.tar.gz
```

### Related Commands

|                                 |                                        |
|---------------------------------|----------------------------------------|
| <a href="#">no</a> on page 1200 | Removes database backup configurations |
|---------------------------------|----------------------------------------|

### *device-onboard*

[Profile Config Commands](#) on page 862

Configures the logo image file name and title displayed on the EGuest device-onboarding portal. The EGuest UI can be accessed only by vendor-admin users.



#### Note

Vendor admin users are configured in the Management policy context. For more information, see [user \(management-policy\)](#) on page 1544.

### Supported in the following platforms:

- Service Platforms — NX9500, NX9510, NX9600, VX9000



## Syntax

```
device-onboard [logo|title] <WORD>
```

## Parameters

```
device-onboard [logo|title] <WORD>
```

|                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>device-onboard</b><br><b>[logo title]</b><br><b>&lt;WORD&gt;</b> | <p>Configures the logo and page title displayed on the device-onboarding portal</p> <ul style="list-style-type: none"><li>• logo - Specify the logo image file name. Note, logo image dimensions must not exceed 109 pixel and 52 pixel in width and height respectively.</li><li>• title - Specify the UI portal title. Note, the title should not exceed 32 characters in length.</li></ul> <p>The following keyword is common to both of the above parameters:</p> <ul style="list-style-type: none"><li>• &lt;WORD&gt; - Specify the logo image file name/page title.</li></ul> |
|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
Split-EG-Server(config-device-00-0C-29-09-3C-CC)#device-onboard logo extremenetworks.png
```

```
Split-EG-Server(config-device-00-0C-29-09-3C-CC)#device-onboard title EXTREME NETWORKS
ONBOARDING UI
```

```
Split-EG-Server(config-device-00-0C-29-09-3C-CC)#show context include-factory | include
device-onboard
device-onboard title EXTREME NETWORKS ONBOARDING UI
device-onboard logo extremenetworks.png
Split-EG-Server(config-device-00-0C-29-09-3C-CC)#
```

Following example shows a Management Policy, vendor-admin user configuration:

```
EC-NOC(config-management-policy-EGuest)#show context include-factory | include user
user onboard-user password 1
1d5e9d60425bde727261b66b5e7eb0236058e7aae45225961ce7b872ea238240 role vendor-admin group
Samsung,Philips,Nest1,Orbit1
EC-NOC(config-management-policy-EGuest)#
```

## Related Commands

|                                 |                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------|
| <a href="#">no</a> on page 1200 | Removes the device-onboarding UI portal's logo image file name and title configuration |
|---------------------------------|----------------------------------------------------------------------------------------|

## *device-upgrade*

[Profile Config Commands](#) on page 862

Configures device firmware upgrade settings on this profile

Administrators can customize profiles with unique device configuration file and firmware upgrade support. In a clustered environment, operations performed on one device are propagated to each member of the cluster and then onwards to devices managed by each cluster member. The number of concurrent device upgrades and their start times can be customized to ensure a sufficient number of devices remain in duty while upgrades are administered to others.

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
device-upgrade [add-auto|auto|count|persist-images]
```

```
device-upgrade add-auto [(ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx9000|nx9600)]
```

```
device-upgrade auto {(ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx9000|nx9600)}
```

```
device-upgrade count <1-128>
```

```
device-upgrade persist-images
```

### Parameters

```
device-upgrade add-auto[(ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx9000|nx9600)]
```

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>device-upgrade</b><br><b>add-auto</b> | Configures a list of device types for automatic firmware upgrade. This command specifies the types of devices that can be automatically upgraded (if enabled). To enable automatic device firmware upgrade, use the 'auto' command. When enabled, access points, wireless controllers, and service platforms, using this profile, will automatically upgrade firmware on adopted devices that match the specified device types. |
| <b>[ &lt;DEVICE-TYPE&gt; ]</b>           | Specifies the type of devices to be upgraded. Select the device type. The options are: AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533, RFS4000, NX5500, NX75XX, NX95XX, NX96XX, VX9000.<br><br><b>Note:</b> Multiple device types can be added to the add-auto list.                                                                                    |

```
device-upgrade auto {(ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx9000|nx9600)}
```

|                            |                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>device-upgrade auto</b> | Enables automatic firmware upgrade on specified device types. When used along with the add-auto command, the auto command allows access points, wireless controllers, and service platforms to automatically upgrade firmware on adopted devices matching the specified device types.                                                                    |
| <b>&lt;DEVICE-TYPE&gt;</b> | Optional. Specifies the type of device to be lined up for automatic firmware upgrade. The options are: AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533, RFS4000, NX5500, NX75XX, NX95XX, NX9600, VX9000.<br><br><b>Note:</b> Multiple device types can be added to the auto list. |

device-upgrade count <1-128>

|                                           |                                                                                                                                                                                    |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>device-upgrade count &lt;1-128&gt;</b> | Configures the maximum number of concurrent upgrades possible <ul style="list-style-type: none"> <li>• &lt;1-128&gt; - specify a value from 1 - 128. The default is 10.</li> </ul> |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

device-upgrade persist-images

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>device-upgrade</b> | Configures parameters for automatic firmware upgrade of adopted devices. Use this command to select the device types and the maximum number of concurrent upgrades.                                                                                                                                                                                                                                                                                                     |
| <b>persist-images</b> | Enables RF Domain manager to retain AP firmware image after upgrade, subject to availability of space. This option is enabled by default.<br>This option is enabled for all controllers and service platforms RF Domain managers with the flash memory capacity to store firmware images for the selected access point models they provision. This feature is disabled for access point RF Domain managers that do not typically have the flash memory capacity needed. |

### Example

```
rfs4000-229D58(config-profile-default-rfs4000)#device-upgrade auto ap7lxx

rfs4000-229D58(config-profile-default-rfs4000)#show context
profile rfs4000 default-rfs4000
 autoinstall configuration
 autoinstall firmware
 device-upgrade auto ap7lxx
 device-upgrade persist-ap-image
 crypto ikev1 policy ikev1-default
 qos trust 802.1p
--More--
rfs4000-229D58(config-profile-default-rfs4000)#
```

### Related Commands

|                                                   |                                                          |
|---------------------------------------------------|----------------------------------------------------------|
| <b>no</b> on page 1200                            | Removes device firmware upgrade settings on this profile |
| <b>device-upgrade</b> on page 726 (show commands) | Displays device upgrade details                          |

*diag*

[Profile Config Commands](#) on page 862

Enables looped packet logging. When enabled, devices, using this profile, start logging looped packets to a separate queue. This option is disabled by default.

Looped packet logging can also be enabled in the device configuration context.



#### Note

To view logged looped packets, execute the **service > show > diag > pkts** command. For more information, see [service](#) on page 647.

#### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
diag pkts
```

#### Parameters

```
diag pkts
```

|                  |                               |
|------------------|-------------------------------|
| <b>diag pkts</b> | Enables looped packet logging |
|------------------|-------------------------------|

#### Example

```
nx9500-6C8809(config-profile-default-nx75xx)#diag pkts
```

```
nx9500-6C8809(config-profile-default-nx75xx)#show context include-factory | include diag
diag pkts
```

```
nx9500-6C8809(config-profile-default-nx75xx)#
```

#### Related Commands

|                                 |                                |
|---------------------------------|--------------------------------|
| <a href="#">no</a> on page 1200 | Disables looped packet logging |
|---------------------------------|--------------------------------|

#### *dot1x*

[Profile Config Commands](#) on page 862

Configures 802.1x standard authentication controls

Dot1x (or 802.1x) is an IEEE standard for network authentication. It enables media-level (layer 2) access control, providing the capability to permit or deny connectivity based on user or device identity. Dot1x allows port-based access using authentication. An dot1x enabled port can be dynamically enabled or disabled depending on user identity or device connection.

Devices supporting dot1x allow the automatic provision and connection to the wireless network without launching a Web browser at login. When within range of a dot1x network, a device automatically connects and authenticates without needing to manually login.

Before authentication, the endpoint is unknown, and traffic is blocked. Upon authentication, the endpoint is known and traffic is allowed. The controller or service platform uses source MAC filtering to ensure only the authenticated endpoint is allowed to send traffic.

Dot1x authentication capabilities is supported on the following platforms:

**Supported in the following platforms:**

- Access Points — AP6522, AP6562, AP7502, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500

Dot1x supplicant capabilities is supported on the following platforms:

**Supported in the following platforms:**

- Access Points — AP6522, AP6562, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500

**Syntax**

```
dot1x [guest-vlan | holdtime | system-auth-control | use]
```

```
dot1x holdtime <0-600>
dot1x system-auth-control
dot1x guest-vlan supplicant
dot1x use aaa-policy <AAA-POLICY-NAME>
```

**Parameters**

```
dot1x system-auth-control
```

|                            |                                                                                                                            |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>system-auth-control</b> | Enables system auth control. Enables dot1x authorization globally for the controller. This feature is disabled by default. |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------|

```
dot1x holdtime <0-600>
```

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>holdtime<br/>&lt;0-600&gt;</b> | Configures a holdtime value. This is the interval after which an authentication attempt is ignored or failed. <ul style="list-style-type: none"><li>• &lt;0-600&gt; – Specify a value from 0 - 600 seconds. A value of '0' indicates no holdtime. The default is 600 seconds or 10 minutes.</li></ul> Adding a hold time at startup allows time for the network to converge before receiving or transmitting 802.1x authentication packets. |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
dot1x guest-vlan supplicant
```



|                   |                                                                                                                               |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>guest-vlan</b> | Configures guest VLAN and supplicant behavior. This feature is disabled by default.                                           |
| <b>supplicant</b> | Allows 802.1x capable supplicant to enter guest VLAN. When enabled, this is the VLAN that supplicant's traffic is bridged on. |

```
dot1x use aaa-policy <AAA-POLICY-NAME>
```

|                                                         |                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>use aaa-policy</b><br><b>&lt;AAA-POLICY-NAME&gt;</b> | Associates a specified 802.1x AAA policy (for MAC authentication) with this access point profile <ul style="list-style-type: none"> <li>• <b>&lt;AAA-POLICY-NAME&gt;</b> - Specify the AAA policy name. Once specified, this AAA policy is utilized for authenticating user requests.</li> </ul> |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Example

```
nx9500-6C8809(config-profile-test-nx5500)#dot1x use aaa-policy OnBoarding
```

```
nx9500-6C8809(config-profile-test-nx5500)#dot1x system-auth-control
```

```
nx9500-6C8809(config-profile-test-nx5500)#show context
profile nx5500 test-nx5500
no autoinstall configuration
no autoinstall firmware
crypto ikev1 policy ikev1-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ikev2 policy ikev2-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
crypto ikev1 remote-vpn
crypto ikev2 remote-vpn
crypto auto-ipsec-secure
crypto load-management
crypto remote-vpn-client
interface ge1
interface ge2
interface ge3
interface ge4
interface ge5
interface ge6
interface pppoe1
use firewall-policy default
service pm sys-restart
router ospf
router bgp
dot1x system-auth-control
dot1x use aaa-policy OnBoarding
nx9500-6C8809(config-profile-test-nx5500)#
```

### Related Commands

|                        |                                               |
|------------------------|-----------------------------------------------|
| <b>no</b> on page 1200 | Disables or reverts settings to their default |
|------------------------|-----------------------------------------------|

*dpi*

[Profile Config Commands](#) on page 862

Enables Deep Packet Inspection (DPI) on this profile. DPI is an advanced packet analysis technique, which analyzes packet and packet content headers to determine the nature of network traffic. When enabled, DPI inspects packets of all flows to identify applications (such as, Netflix, Twitter, Facebook,

etc.) and extract metadata (such as, host name, server name, TCP-RTT, etc.) for further use by the WiNG firewall.

This command is also available in the device configuration mode.

#### Supported in the following platforms:

- Access Points — AP7522, AP7532, AP7602, AP7612, AP7622, AP7632, AP7662
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

#### Syntax

```
dpi {custom-app/logging/metadata}
```

```
dpi {custom-app <CUSTOM-APP-NAME>}
```

```
dpi {logging [level [<0-7>|alerts|critical|debugging|emergencies|errors|informational|notifications|warnings]|on]}
```

```
dpi {metadata [http/ssl/tcp-rtt/voice-video]}
```

```
dpi {metadata [http/ssl/voice-video]}
```

```
dpi {metadata tcp-rtt {app-group <APPLICATION-GROUP-NAME>}}
```

#### Parameters

```
dpi {custom-app <CUSTOM-APP-NAME>}
```

|                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>dpi</b>                                    | Enables DPI on this profile/device context and configures DPI settings. When enabled, all flow traffic is subjected to DPI for detection of applications, application categories, custom applications, and metadata extraction.                                                                                                                                                                                                    |
| <b>custom-app<br/>&lt;CUSTOM-APP-NAME&gt;</b> | Optional. Adds custom application to this profile <ul style="list-style-type: none"><li>• &lt;CUSTOM-APP-NAME&gt; – Specify custom application name (should be existing and configured)</li></ul> If no custom application is specified, the system detects the PACE built-in applications.<br><b>Note:</b> For more information on application categories and application detection, see <a href="#">application</a> on page 258. |

```
dpi {logging [level [<0-7>|alerts|critical|debugging|emergencies|errors|informational|notifications|warnings]|on]}
```

|                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>dpi</b>                                                                                                                                    | Enables DPI on this profile/device context and configures DPI settings. When enabled, all flow traffic is subjected to DPI for detection of applications, application categories, custom applications, and metadata extraction.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>logging [level [ &lt;0-7&gt;   alerts   critical   debugging   emergencies   errors   informational   notifications   warnings ]   on]</b> | <p>Optional. Enables DPI logging and sets the logging level</p> <ul style="list-style-type: none"> <li>level – Configures the DPI logging level. Use one of the following options to specify the logging level: <ul style="list-style-type: none"> <li>&lt;0-7&gt; Logging severity level</li> <li>alerts Immediate action needed (1)</li> <li>critical Critical conditions (2)</li> <li>debugging Debugging messages (7)</li> <li>emergencies System is unusable (0)</li> <li>errors Conditions (3)</li> <li>informational Informational messages (6)</li> <li>notifications Normal but significant conditions (5) - Default setting</li> <li>warnings Warning conditions (4)</li> </ul> </li> </ul> <p>Either specify the logging level index (from 0 - 7) or the description. For example, to log all alerts either enter '1' or 'alerts'.</p> <ul style="list-style-type: none"> <li>on – Enables application detection event logging. DPI logging is disabled by default.</li> </ul> |

```
dpi {metadata [http|ssl|voice-video]}
```

|                                        |                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| • <b>dpi</b>                           | Enables DPI on this profile/device context and configures DPI settings. When enabled, all flow traffic is subjected to DPI for detection of applications, application categories, custom applications, and metadata extraction.                                                                                                        |
| <b>metadata [http ssl voice-video]</b> | <p>Optional. Enables metadata extraction from following flows:</p> <ul style="list-style-type: none"> <li>http – HTTP flows. This option is disabled by default.</li> <li>ssl – SSL flows. This option is disabled by default.</li> <li>voice-video – Voice and video classified flows. This option is disabled by default.</li> </ul> |

```
dpi {metadata tcp-rtt {app-group <APPLICATION-GROUP-NAME>}}
```

|                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>dpi</b>                                                         | Enables DPI on this profile/device context and configures DPI settings. When enabled, all flow traffic is subjected to DPI for detection of applications, application categories, custom applications, and metadata extraction.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>metadata tcp-rtt {app-group &lt;APPLICATION-GROUP-NAME&gt;}</b> | <p>Optional. Enables Transmission Control Protocol - Round Trip Time (TCP-RTT) metadata collection for application groups. Before executing this command, ensure that you have created at least one application group.</p> <p>Enable this option in the profile/device contexts of the AP7522, AP7532, AP7562, AP8432, AP8533 access point models, as only these APs support TCP-RTT metadata collection.</p> <ul style="list-style-type: none"> <li>app-group – Optional. Specifies the customized application-group name containing the applications for which TCP-RTT is to be collected <ul style="list-style-type: none"> <li>&lt;APPLICATION-GROUP-NAME&gt; – Specify the app-group name (should be existing and configured). If not specified, the system collects TCP-RTT metadata for all the customized app-groups created. You can enable TCP-RTT metadata collection on eight (8) application groups at a time.</li> </ul> </li> </ul> <p>For more information on creating customized application-groups, see <a href="#">application-group</a> on page 263.</p> <p>The TCP-RTT metadata is viewable only on the NSight dashboard. Therefore, ensure the NSight server and database is up and NSight analytics data collection is enabled.</p> |



## Example

```
nx9500-6C8809(config-profile-testNX9500)#dpi logging on

nx9500-6C8809(config-profile-testNX9500)#dpi logging level 7

nx9500-6C8809(config-profile-testNX9500)#show context
profile nx9000 testNX9500
 bridge vlan 10
 ip igmp snooping
 ip igmp snooping querier
 ipv6 mld snooping

 router bgp
 dpi logging on
 dpi logging level debugging
nx9500-6C8809(config-profile-testNX9500)#

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#dpi metadata tcp-rtt app-group amazon
```

## Related Commands

|                                 |                                                      |
|---------------------------------|------------------------------------------------------|
| <a href="#">no</a> on page 1200 | Disables DPI (application assurance) on this profile |
|---------------------------------|------------------------------------------------------|

### *dscp-mapping*

[Profile Config Commands](#) on page 862

Configures IP Differentiated Services Code Point (DSCP) to 802.1p priority mapping for untagged frames

#### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
dscp-mapping <WORD> priority <0-7>
```

#### Parameters

```
dscp-mapping <word> priority <0-7>
```

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;WORD&gt;</b>         | Specifies the DSCP value of a received IP packet. This could be a single value or a list. For example, 10-20, 25, 30-35.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>priority &lt;0-7&gt;</b> | <p>Specifies the 802.1p priority to use for a packet if untagged. The priority is set on a scale of 0 - 7. The priority values are:</p> <ul style="list-style-type: none"> <li>• 0 - Best effort</li> <li>• 1 - Background</li> <li>• 2 - Spare</li> <li>• 3 - Excellent effort</li> <li>• 4 - Controlled load</li> <li>• 5 - Video</li> <li>• 6 - Voice</li> <li>• 7 - Network control</li> </ul> <p><b>Note:</b> The specified 802.1p priority value is added as a 3-bit IP precedence value in the Type of Service (ToS) field of the IP header used to set the priority. Up to 64 entries are permitted.</p> |

### Example

```
nx9500-6C8809(config-profile-default-rfs4000)#dscp-mapping 20 priority 7
```

```
nx9500-6C8809(config-profile-default-rfs4000)#show context
profile rfs7000 default-rfs4000
dscp-mapping 20 priority 7
no autoinstall configuration
no autoinstall firmware
crypto isakmp policy default
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
interface mel
interface gel
ip dhcp trust
qos trust dscp
nx9500-6C8809(config-profile-default-rfs4000)#
```

### Related Commands

|                        |                                               |
|------------------------|-----------------------------------------------|
| <b>no</b> on page 1200 | Disables or reverts settings to their default |
|------------------------|-----------------------------------------------|

*eguest-server (VX9000 only)*

[Profile Config Commands](#) on page 862

Enables the ExtremeGuest (EGuest) server

The WiNG EGuest solution is an independently installable VM/Server that provides integrated guest management and analytics. Use this command to enable the EGuest daemon on the EGuest server.



#### Note

EGuest being a licensed feature, ensure that the EGUEST-DEV license is applied on the EGuest server's self context. For more information, see [license](#) on page 1267.

---

### Supported in the following platforms:

- Service Platforms — VX9000



#### Note

For more information on configuring an EGuest captive-portal deployment, see [configuring ExtremeGuest captive portal](#) on page 332.

---

### Syntax

```
eguest-server
```

### Parameters

```
eguest-server
```

|                      |                                                                                                                                                                                                         |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>eguest-server</b> | <b>Note:</b> Execute this command, without the 'host' option, on the EGuest server. When executed, the EGuest daemon is enabled on the host.<br><br>EGuest server can be hosted only a VX9000 platform. |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Example

On the EGuest server, execute the command without the 'host' option to enable the EGuest daemon.

```
EG-Server(config-device-02-EE-1A-7E-AE-5B)#eguest-server
```

```
EG-Server(config-device-02-EE-1A-7E-AE-5B)#show context include-factory | include eguest-server
eguest-server
EG-Server(config-device-02-EE-1A-7E-AE-5B)#
```

### Related Commands

|                                 |                                                          |
|---------------------------------|----------------------------------------------------------|
| <a href="#">no</a> on page 1200 | Disables the EGuest server by stopping the EGuest daemon |
|---------------------------------|----------------------------------------------------------|

*eguest-server (NOC Only)*

[Profile Config Commands](#) on page 862

Points to the EGuest server when executed along with the 'host' option. The WiNG EGuest solution is an independently installable VM/Server that provides integrated guest management and analytics. Use this command to enable the EGuest daemon on the EGuest server.



#### Note

EGuest being a licensed feature, ensure that the EGUEST-DEV license is applied on the EGuest server's self context. For more information, see [license](#) on page 1267.

---

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000

- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000



#### Note

For more information on configuring an EGuest captive-portal deployment, see [configuring ExtremeGuest captive portal](#) on page 332.

#### Syntax

```
eguest-server <1-3> host <IPv4/IPv6/HOSTNAME> {http|https}
```

#### Parameters

```
eguest-server <1-3> host <IPv4/IPv6/HOSTNAME> {http|https}
```

|                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>eguest-server</b><br/> <b>&lt;1-3&gt; host</b><br/> <b>&lt;IPv4/IPv6/</b><br/> <b>HOSTNAME&gt;</b><br/> <b>{http https}</b></p> | <p>Configures the EGuest server details in the profile/device context of the NOC (access point/controller). When configured, the NOC posts registration requests and captive-portal related data directly to the specified EGuest server.</p> <ul style="list-style-type: none"> <li>• &lt;1-3&gt; - Configures the EGuest server index number. A maximum of three EGuest servers can be configured.</li> <li>• host &lt;IPv4/IPv6/HOSTNAME&gt; - Configures the EGuest server's IPv4/IPv6 address or hostname. <ul style="list-style-type: none"> <li>{http https} - Optional. Configures the mode of connection as HTTP or HTTPS.</li> </ul> </li> </ul> <p><b>Note:</b> HTTPS is recommended as it uses encryption for transmission and is therefore more secure.</p> |
|---------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Example

On the NOC, execute along with the 'host' option to point to the EGuest server.

```
EG-NOC(config-device-74-67-F7-5C-64-4A)#eguest-server 1 host EG-Server https

EG-NOC(config-device-74-67-F7-5C-64-4A)#show context include-factory | include eguest-server
no eguest-server
eguest-server 1 host EG-Server https
EG-NOC(config-device-74-67-F7-5C-64-4A)#
```

#### Related Commands

|                                 |                                                             |
|---------------------------------|-------------------------------------------------------------|
| <a href="#">no</a> on page 1200 | Removes the EGuest server IP address/hostname configuration |
|---------------------------------|-------------------------------------------------------------|

#### *email-notification*

[Profile Config Commands](#) on page 862

Configures e-mail notification settings. When a system event occurs e-mail notifications are sent (provided message logging is enabled) based on the settings configured here. Use this option to configure the outgoing SMTP server settings.

#### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
email-notification [host|recipient]
```

```
email-notification recipient <RECIPIENT-NAME>
```

```
email-notification host <SMTP-SERVER-IP/HOSTNAME> sender <SENDER-EMAIL>
[port|security|username]
```

```
email-notification host <SMTP-SERVER-IP/HOSTNAME> sender <SENDER-EMAIL>
[(port <1-65535>, security [none|ssl|starttls], username <SMTP-USERNAME>
password [2 <WORD>|<WORD>])]
```

### Parameters

```
email-notification recipient <RECIPIENT-EMAIL>
```

|                                                    |                                                                                                                                                                                                                                                                           |
|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>recipient</b><br><b>&lt;RECIPIENT-EMAIL&gt;</b> | <p>Defines the recipient's e-mail address. A maximum of 6 (six) e-mail addresses can be configured.</p> <ul style="list-style-type: none"> <li>• &lt;RECIPIENT-EMAIL&gt; - Specify the recipient's e-mail address (should not exceed 64 characters in length).</li> </ul> |
|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
email-notification host <SMTP-SERVER-IP/HOSTNAME> sender <SENDER-EMAIL> [(port <1-65535>,
security [none|ssl|starttls], username <SMTP-USERNAME> password [2 <WORD>|<WORD>])]
```

|                                             |                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>host &lt;SMTP-SERVER-IP/HOSTNAME&gt;</b> | <p>Configures the host SMTP server's IP address or hostname</p> <ul style="list-style-type: none"> <li>• &lt;SMTP-SERVER-IP/HOSTNAME&gt; - Specify the SMTP server's IP address or hostname.</li> </ul>                                                                                                                                                                      |
| <b>sender &lt;SENDER-EMAIL&gt;</b>          | <p>Defines the sender's e-mail address. This is the from address on notification e-mails.</p> <ul style="list-style-type: none"> <li>• &lt;SENDER-EMAIL&gt; - Specify the sender's e-mail address (should not exceed 64 characters in length). Use the email-notification &gt; recipient &gt; &lt;EMAIL-ADDRESS&gt; command to configure the recipient's address.</li> </ul> |
| <b>port &lt;1-65535&gt;</b>                 | <p>This option is recursive and applicable to the 'security' and 'username' parameters. Configures the SMTP server port. Use this option to configure a non-standard SMTP port on the outgoing SMTP server. The standard SMTP port is 25.</p> <ul style="list-style-type: none"> <li>• &lt;1-65535&gt; - Specify the port from 1 - 65535.</li> </ul>                         |

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>security</b> [none   ssl   starttls] | <p>This option is recursive and applicable to the 'port' and 'username' parameters. Configures the SMTP encryption type used</p> <ul style="list-style-type: none"> <li>• none – No encryption used</li> <li>• ssl – Uses Secure Sockets Layer (SSL) encryption between the SMTP server and the client</li> <li>• starttls – Uses STARTTLS encryption between the SMTP server and the client</li> </ul> |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>username</b> <SMTP-USERNAME><br><b>password</b> [ 2 <WORD>   <WORD> ] | <p>This option is recursive and applicable to the 'port' and 'security' parameters. Configures the SMTP sender's username. Many SMTP servers require users to authenticate with a username and password before sending e-mail through the server.</p> <ul style="list-style-type: none"> <li>• &lt;SMTP-USERNAME&gt; – Specify the SMTP username (should not exceed 64 characters in length).</li> <li>• password – Configures the SMTP server password. Specify the password associated with the username of the sender on the outgoing SMTP server. <ul style="list-style-type: none"> <li>2 &lt;WORD&gt; – Configures an encrypted password</li> <li>&lt;WORD&gt; – Specify the password (should not exceed 127 characters in length).</li> </ul> </li> </ul> |
|--------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Example**

```

nx9500-6C8809(config-profile-default-rfs4000)#email-notification recipient
test@examplecompany.com

nx9500-6C8809(config-profile-default-rfs4000)#show context
profile rfs4000 default-rfs4000
dscp-mapping 20 priority 7
no autoinstall configuration
no autoinstall firmware
.....
interface ge4
ip dhcp trust
qos trust dscp
qos trust 802.1p
use firewall-policy default
email-notification recipient test@examplecompany.com
service pm sys-restart
nx9500-6C8809(config-profile-default-rfs4000)#

```

**Related Commands**

|                        |                                               |
|------------------------|-----------------------------------------------|
| <b>no</b> on page 1200 | Disables or reverts settings to their default |
|------------------------|-----------------------------------------------|

*enforce-version*

[Profile Config Commands](#) on page 862

Enables checking of a device's firmware version before attempting adoption or clustering

**Supported in the following platforms:**

- Access Points — AP6522, AP6562, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

## Syntax

```
enforce-version [adoption|cluster] [full|major|minor|none|strict]
```

## Parameters

```
enforce-version [adoption|cluster] [full|major|minor|none|strict]
```

|                 |                                                                                                                                                                            |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>adoption</b> | Verifies firmware versions before adopting. This option is enabled by default.                                                                                             |
| <b>cluster</b>  | Verifies firmware versions before clustering. This option is enabled by default.                                                                                           |
| <b>full</b>     | Allows adoption or clustering when the first four octets of the firmware versions match (for example 5.8.6.0)                                                              |
| <b>major</b>    | Allows adoption or clustering when the first two octets of the firmware versions match (for example 5.8)                                                                   |
| <b>minor</b>    | Allows adoption or clustering when the first three octets of the firmware versions match (for example 5.8.6)                                                               |
| <b>none</b>     | Allows adoption or clustering between any firmware versions                                                                                                                |
| <b>strict</b>   | Allows adoption or clustering only when firmware versions exactly match (for example 5.8.6.0-008B). This is the default setting for both 'adoption' and 'cluster' options. |

## Example

```
nx9500-6C8809(config-profile-test-nx5500)#enforce-version cluster full
nx9500-6C8809(config-profile-test-nx5500)#enforce-version adoption major
```

```
nx9500-6C8809(config-profile-test-nx5500)#show context
profile nx5500 test-nx5500
 no autoinstall configuration
 no autoinstall firmware
 crypto ikev1 policy ikev1-default
 isakmp-proposal default encryption aes-256 group 2 hash sha

interface pppoel
 use firewall-policy default
 enforce-version adoption major
 enforce-version cluster full
 service pm sys-restart
 router ospf
 router bgp
 dot1x system-auth-control
 dot1x use aaa-policy OnBoarding
nx9500-6C8809(config-profile-test-nx5500)#
```

## Related Commands

|                                 |                                               |
|---------------------------------|-----------------------------------------------|
| <a href="#">no</a> on page 1200 | Disables or reverts settings to their default |
|---------------------------------|-----------------------------------------------|

*environmental-sensor*

[Profile Config Commands](#) on page 862

Configures the environmental sensor settings

An AP8132 sensor module is a USB environmental sensor extension to an AP8132 model access point. It provides a variety of sensing mechanisms, allowing the monitoring and reporting of the AP8132's radio coverage area.

**Supported in the following platforms:**

- Access Points – AP8132

**Syntax**

```
environmental-sensor [humidity|light|motion|polling-interval|temperature]
```

```
environmental-sensor [humidity|motion|polling-interval <1-100>|
temperature]
```

```
environmental-sensor light {holdtime|radio-shutdown|threshold}
```

```
environmental-sensor light {holdtime <10-201>|radio-shutdown [all|
radio-1|radio-2]}
```

```
environmental-sensor light {threshold [high <100-10000>|low <0-1000>]}
```

**Parameters**

```
environmental-sensor [humidity|motion|polling-interval <1-100>|temperature]
```

|                                       |                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>environmental-sensor</b>           | Configures environmental sensor settings on this profile                                                                                                                                                                                                                                                                         |
| <b>humidity</b>                       | Enables (turns on) humidity sensors. This setting is enabled by default.                                                                                                                                                                                                                                                         |
| <b>motion</b>                         | Enables (turns on) motion sensors. This setting is enabled by default.                                                                                                                                                                                                                                                           |
| <b>polling-interval &lt;1-100&gt;</b> | Configures polling interval, in seconds, on all sensors. This is the interval after which the sensor module polls its environment to assess the various parameters, such as light intensity. <ul style="list-style-type: none"> <li>• &lt;1-100&gt; – Specify a value from 1 - 100 seconds. The default is 5 seconds.</li> </ul> |
| <b>temperature</b>                    | Enables (turns on) temperature sensors. This setting is enabled by default.                                                                                                                                                                                                                                                      |

```
environmental-sensor light {holdtime <10-201>|radio-shutdown [all|radio-1|radio-2]}
```

|                             |                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>environmental-sensor</b> | Configures environmental sensor settings on this profile                                                                                                                                                                                                                                                                                                                                   |
| <b>light</b>                | Enables (turns on) light sensors and specifies its settings<br>When enabled, the sensor module polls the environment to determine the light intensity. Based on the reading, the system determines whether the AP8132's deployment location has lights on or off. Light intensity also helps determine whether the access point's deployment location is currently populated with clients. |



|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>holdtime</b><br><b>&lt;10-201&gt;</b>                | Optional. Configures a holdtime, in seconds, for the light sensor <ul style="list-style-type: none"> <li>• &lt;10-201&gt; - Specify a value from 10 - 201 seconds. The default value is 11 seconds.</li> </ul>                                                                                                                                                                                                                                                               |
| <b>radio-shutdown</b><br><b>[all   radio1   radio2]</b> | Optional. Shuts down the sensor's radios <ul style="list-style-type: none"> <li>• all - Shuts down all radios. This is the default setting.</li> <li>• radio1 - Shuts down radio 1</li> <li>• radio2 - Shuts down radio 2</li> </ul> <p>AP8132's using this profile have their radios shut down, when the radio's power falls below the specified threshold. Use the environmental-sensor &gt; light &gt; threshold &gt; [high low] command to set the threshold values.</p> |

```
environmental-sensor light {threshold [high <100-10000>|low <0-1000>]}
```

|                                         |                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>environmental-sensor</b>             | Configures environmental sensor settings on this profile                                                                                                                                                                                                                                                                                         |
| <b>light</b>                            | Enables (turns on) light sensors and specifies its settings                                                                                                                                                                                                                                                                                      |
| <b>threshold</b>                        | Optional. Configures the upper and lower thresholds for the amount of light in the environment                                                                                                                                                                                                                                                   |
| <b>high</b><br><b>&lt;100-10000&gt;</b> | Specifies the upper threshold from 100 - 10000 lux. This value determines whether lighting is on in the AP8132's deployment location. The radios are turned off if the average reading value is lower than the value set here. The default is 400 lux.<br>The light sensor triggers an event if the amount of light exceeds the specified value. |
| <b>low</b> <b>&lt;0-1000&gt;</b>        | Specifies the lower threshold from 0 - 1000 lux. This value determines whether lighting is off in the AP8132's deployment location. The radios are turned on when the average value is higher than the value set here. The default is 200 lux.<br>The light sensor triggers an event if the amount of light drops below the specified value.     |

### Example

```
rfs4000-229D58(config-profile-testRFS4000)#environmental-sensor humidity
rfs4000-229D58(config-profile-testRFS4000)#environmental-sensor polling-interval 60
rfs4000-229D58(config-profile-testRFS4000)#environmental-sensor light radio-shutdown all
rfs4000-229D58(config-profile-testRFS4000)#environmental-sensor light threshold high 300
rfs4000-229D58(config-profile-testRFS4000)#environmental-sensor light threshold low 100
```

```
rfs4000-229D58(config-profile-testRFS4000)#show context
profile rfs4000 testRFS4000
 bridge vlan 1
 tunnel-over-level2
 ip igmp snooping
 ip igmp snooping querier
 environmental-sensor polling-interval 60
 environmental-sensor light threshold high 300
 environmental-sensor light threshold low 100
 environmental-sensor light radio-shutdown all
 no autoinstall configuration
 no autoinstall firmware
 device-upgrade persist-images
--More--
rfs4000-229D58(config-profile-testRFS4000)#
```

### Related Commands

|                        |                                             |
|------------------------|---------------------------------------------|
| <b>no</b> on page 1200 | Removes the environmental sensor's settings |
|------------------------|---------------------------------------------|

## events

[Profile Config Commands](#) on page 862

Displays system event messages

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
events [forward on|on]
```

### Parameters

```
events [forward on|on]
```

|                   |                                                                                                                                                                                                                                 |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>forward on</b> | Forwards system event messages to the wireless controller, service platform, or cluster members. This feature is enabled by default. <ul style="list-style-type: none"><li>• on – Enables forwarding of system events</li></ul> |
| <b>on</b>         | Generates system events. This feature is enabled by default.                                                                                                                                                                    |

### Example

```
nx9500-6C8809(config-profile-default-rfs4000)#events forward on
nx9500-6C8809(config-profile-default-rfs4000)#
```

### Related Commands

|                           |                                               |
|---------------------------|-----------------------------------------------|
| <b>no on</b> on page 1200 | Disables or reverts settings to their default |
|---------------------------|-----------------------------------------------|

## export

[Profile Config Commands](#) on page 862

Enables export of startup.log file after every boot

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
export startup-log [max-retries|retry-interval|url]
export startup-log [max-retries <2-65535>|retry-interval <30-86400>|url
<URL>]
```

## Parameters

`export startup-log [max-retries <2-65535>|retry-interval <30-86400>|url <URL>]`

|                                        |                                                                                                                                                                                                          |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>export startup-log</b>              | Enables export of the startup.log file after every boot. This option is disabled by default.                                                                                                             |
| <b>max-retries &lt;2-65535&gt;</b>     | Configures the maximum number of retries in case the export process fails <ul style="list-style-type: none"><li>• &lt;2-65535&gt; - Specify a value from 2 - 65535.</li></ul>                            |
| <b>retry-interval &lt;30-86400&gt;</b> | Configures the interval between two consecutive retries <ul style="list-style-type: none"><li>• &lt;30-86400&gt; - Specify a value from 30 - 86400 seconds.</li></ul>                                    |
| <b>url &lt;URL&gt;</b>                 | Configures the destination URL in the following format:<br>tftp://<hostname IP>[:port]/path/file<br>ftp://<user>:<passwd>@<hostname IP>[:port]/path/file<br>sftp://<user>@<hostname IP>[:port]/path/file |

## Example

```
nx9500-6C8809(config-profile-test-nx5500)#export startup-log max-retries 10 retry-interval 30 url ftp://anonymous:anonymous@192.168.13.10/log/startup.log
```

```
nx9500-6C8809(config-profile-test-nx5500)#show context
profile nx5500 test-nx5500
 no autoinstall configuration
 no autoinstall firmware
 crypto ikev1 policy ikev1-default

 interface ge5
 interface ge6
 interface pppoe1
 use firewall-policy default
 export startup-log max-retries 10 retry-interval 30 url ftp://
anonymous:anonymous@192.168.13.10/log/startup.log
 enforce-version adoption major
 enforce-version cluster full
 service pm sys-restart
--More--
nx9500-6C8809(config-profile-test-nx5500)#
```

## Related Commands

|                              |                                     |
|------------------------------|-------------------------------------|
| <code>no</code> on page 1200 | Disables export of startup.log file |
|------------------------------|-------------------------------------|

## *file-sync*

[Profile Config Commands](#) on page 862

Configures parameters enabling auto syncing of trustpoint/wireless-bridge certificate between the staging-controller and its adopted access points

This command is applicable to the access point's profile as well as device configuration modes.

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000

- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

### Syntax

```
file-sync [auto|count <1-20>]
```

### Parameters

```
file-sync [auto|count <1-20>]
```

|                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>file-sync</b><br><b>[auto count</b><br><b>&lt;1-20&gt;]</b> | <p>Configures the following file-synching parameters:</p> <ul style="list-style-type: none"> <li>• auto - Enables the staging controller to autoinstall trustpoint/wireless-bridge certificate on an access point when it comes up for the first time and adopts to the controller.</li> </ul> <p>Prior to enabling file syncing, ensure that the wireless-bridge certificate is present on the staging controller. To upload the certificate on the controller, in the user or privilege executable modes, execute the following command:<br/>file-sync &gt; load-file &gt; &lt;URL&gt;.</p> <ul style="list-style-type: none"> <li>• count &lt;1-20&gt; - Configures the maximum number of access points that can be concurrently auto-installed. <ul style="list-style-type: none"> <li>• &lt;1-20&gt; - Specify a value from 1 - 20. The default is 10 access points.</li> </ul> </li> </ul> <p><b>Note:</b> For the NX95XX service platforms the count-range is from 1 - 128.</p> |
|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
nx9500-6C8809(config-profile-default-rfs4000)#file-sync auto
```

```
nx9500-6C8809(config-profile-default-rfs4000)#file-sync count 8
```

```
nx9500-6C8809(config-profile-default-rfs4000)#show context
profile rfs4000 default-rfs4000
no autoinstall configuration
no autoinstall firmware
no device-upgrade auto
file-sync count 8
file-sync auto
crypto ikev1 policy ikev1-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ikev2 policy ikev2-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
--More--
nx9500-6C8809(config-profile-default-rfs4000)#
```

### Related Commands

|                        |                                                                                      |
|------------------------|--------------------------------------------------------------------------------------|
| <b>no</b> on page 1200 | Disables automatic file syncing between the staging-controller and its access points |
|------------------------|--------------------------------------------------------------------------------------|

*floor*

[Profile Config Commands](#) on page 862

Sets the floor name where the target device (access point, wireless controller, or service platform using this profile) is physically located. Assigning a building floor name helps in grouping devices within the same general coverage area.

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
floor <WORD> {<1-4094>}
```

### Parameters

```
floor <WORD> {<1-4094>}
```

|                                                      |                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>floor &lt;WORD&gt;</b><br><b>{&lt;1-4094&gt;}</b> | Sets the floor name where the target device is located <ul style="list-style-type: none"><li>• &lt;WORD&gt; - Specify the floor name (should not exceed 64 characters in length).</li><li>• &lt;1-4094&gt; - Optional. Configures the floor number from 1 - 4094. The default is 1.</li></ul> |
|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Example

```
nx9500-6C8809(config-profile-default-rfs4000)#floor fifth

nx9500-6C8809(config-profile-default-rfs4000)#show context
profile rfs4000 default-rfs4000
 bridge vlan 1
 ip igmp snooping
 ip igmp snooping querier
 area Ecospace
 floor fifth
 autoinstall configuration
 autoinstall firmware
--More--
nx9500-6C8809(config-profile-default-rfs4000)#
```

### Related Commands

|                        |                                             |
|------------------------|---------------------------------------------|
| <b>no</b> on page 1200 | Resets the configured floor name and number |
|------------------------|---------------------------------------------|

*gre*

[Profile Config Commands](#) on page 862

The following table summarizes commands that allow you to enter the GRE configuration mode:

| Command                                          | Description                                                                                                                                                                        |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">gre</a> on page 1002                 | Enables GRE tunneling on a profile/device. This command also creates a GRE tunnel and enters its configuration mode. Use this command to modify an existing GRE tunnel's settings. |
| <a href="#">gre-config-instance</a> on page 1003 | Summarizes GRE tunnel configuration mode commands                                                                                                                                  |

## gre

gre on page 1001

Enables Generic Routing Encapsulation (GRE) tunneling on this profile, and creates a new GRE tunnel or modifies an existing GRE tunnel.

The GRE protocol allows encapsulation of one protocol over another. It is a tunneling protocol that transports any layer 3 protocol over an IP network. When enabled, a payload packet is first encapsulated in the GRE protocol. The GRE encapsulated payload is then encapsulated in another IP packet before being forwarded to the destination.

GRE tunneling can be configured to bridge Ethernet packets between WLANs and a remote WLAN gateway over an IPv4 GRE tunnel. The tunneling of 802.3 packets using GRE is an alternative to MiNT or L2TPv3. Related features like ACLs for extended VLANs are still available using layer 2 tunneling over GRE.

Using GRE, access points map one or more VLANs to a tunnel. The remote end point is a user-configured WLAN gateway IP address, with an optional secondary IP address should connectivity to the primary GRE peer be lost. VLAN traffic is expected in both directions in the GRE tunnel. A WLAN mapped to these VLANs can be either open or secure. Secure WLANs require authentication to a remote RADIUS server available within your deployment using standard RADIUS protocols. Access Points can reach both the GRE peer as well as the RADIUS server using IPv4.

The WiNG software now supports for both IPv4 or IPv6 tunnel endpoints. However, a tunnel needs to contain either IPv4 or IPv6 formatted device addresses and cannot be mixed. With the new IPv6 tunnel implementation, all outbound packets are encapsulated with the GRE header, then the IPv6 header. The header source IP address is the local address of the IPv6 address of tunnel interface, and the destination address peer address of the tunnel. All inbound packets are de-capsulated by removing the IPv6 and GRE header before sending it over to the IP stack.



### Note

Only one GRE tunnel can be created for every profile.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
gre tunnel <GRE-TUNNEL-NAME>
```

Parameters

```
gre tunnel <GRE-TUNNEL-NAME>
```

|                                                     |                                                                                                                                                                                                                                                    |
|-----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>gre tunnel</b><br><b>&lt;GRE-TUNNEL-NAME&gt;</b> | Creates a new GRE tunnel or modifies an existing GRE tunnel <ul style="list-style-type: none"><li>• &lt;GRE-TUNNEL-NAME&gt; – If creating a new tunnel, specify a unique name for it. If modifying an existing tunnel, specify its name.</li></ul> |
|-----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Example

```
rfs4000-229D58(config-profile testRFS4000-gre-tunnel-testGREtunnel)#?
GRE Tunnel Mode commands:
 dscp Differentiated Services Code Point
 establishment-criteria Set tunnel establishment criteria
 failover L2gre tunnel failover
 mtu L2GRE tunnel endpoint maximum transmission unit(MTU)
 native Native trunking characteristics
 no Negate a command or set its defaults
 peer L2GRE peer
 tunneled-vlan VLANs to tunnel

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

rfs4000-229D58(config-profile testRFS4000-gre-tunnel-testGREtunnel)#

rfs4000-229D58(config-profile testRFS4000-gre-tunnel-testGREtunnel)#peer 1 ip 192.168.13.8
rfs4000-229D58(config-profile testRFS4000-gre-tunnel-testGREtunnel)#peer 2 ip 192.168.13.10

rfs4000-229D58(config-profile testRFS4000-gre-tunnel-testGREtunnel)#show context
gre tunnel testGREtunnel
 peer 1 ip 192.168.13.8
 peer 2 ip 192.168.13.10
rfs4000-229D58(config-profile testRFS4000-gre-tunnel-testGREtunnel)#

rfs4000-229D58(config-profile-testRFS4000)#show context
profile rfs4000 testRFS4000
 bridge vlan 1
 tunnel-over-level2
 ip igmp snooping
 ip igmp snooping querier
.....
use firewall-policy default
service pm sys-restart
router ospf
gre tunnel testGREtunnel
 peer 1 ip 192.168.13.8
 peer 2 ip 192.168.13.10
rfs4000-229D58(config-profile-testRFS4000)#
```

## Related Commands

|                                 |                                        |
|---------------------------------|----------------------------------------|
| <a href="#">no</a> on page 1200 | Disables GRE tunneling on this profile |
|---------------------------------|----------------------------------------|

## gre-config-instance

[gre](#) on page 1001

The following table summarizes GRE tunnel configuration mode commands:

| Command                                             | Description                                                                                             |
|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| <a href="#">dscp</a> on page 1004                   | Sets the GRE tunnel's Differentiated Services Code Point (DSCP) / 802.1q priority value                 |
| <a href="#">establishment-criteria</a> on page 1005 | Configures the GRE tunnel establishment criteria                                                        |
| <a href="#">failover</a> on page 1005               | Enables periodic pinging of the primary gateway to assess its availability, in case it is unreachable   |
| <a href="#">mtu</a> on page 1006                    | Configures the maximum transmission unit (MTU) for IPv4/IPv6 L2GRE tunnel endpoints                     |
| <a href="#">native</a> on page 1007                 | Configures native trunking settings for this GRE tunnel                                                 |
| <a href="#">no</a> on page 1008                     | Removes the GRE tunnel settings based on the parameters passed                                          |
| <a href="#">peer</a> on page 1009                   | Configures the GRE tunnel's end-point peers                                                             |
| <a href="#">tunneled-vlan</a> on page 1010          | Defines the VLAN that connected clients use to route GRE-tunneled traffic within their respective WLANs |

dscp

[gre-config-instance](#) on page 1003

Sets the GRE tunnel's DSCP / 802.1q priority value from encapsulated packets to the outer packet IPv4 header.

This option is disabled by default.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

**dscp** [**<0-63>** | **reflect**]

Parameters

**dscp** [**<0-63>** | **reflect**]

|                                 |                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------|
| <b>dscp</b> <b>&lt;0-63&gt;</b> | Specifies the DSCP 802.1q priority value for outer packets from 0 - 63. The default is 1. |
| <b>dscp</b> <b>reflect</b>      | Copies the DSCP 802.1q value from inner packets                                           |

Example

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGREtunnel)#dscp 20

rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGREtunnel)#show context
 gre tunnel testGREtunnel
 dscp 20
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGREtunnel)#
```

Related Commands

|                                 |                                                                |
|---------------------------------|----------------------------------------------------------------|
| <a href="#">no</a> on page 1008 | Removes the GRE tunnel settings based on the parameters passed |
|---------------------------------|----------------------------------------------------------------|



establishment-criteria

[gre-config-instance](#) on page 1003

Configures the GRE tunnel establishment criteria

In a multi-controller RF domain, it is always the master node that establishes the tunnel. The tunnel is created only if the tunnel device is designated as one of the following: vrrp-master, cluster-master, or rf-domain-manager.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
establishment-criteria [always | cluster-master | rf-domain-manager | vrrp-master <1-255>]
```

Parameters

```
establishment-criteria [always | cluster-master | rf-domain-manager | vrrp-master <1-255>]
```

|                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>establishment-criteria</b><br><b>[always   cluster-master   rf-domain-manager   vrrp-master &lt;1-255&gt;]</b> | Configures the GRE tunnel establishment criteria. The options are: <ul style="list-style-type: none"><li>• always – Always automatically establishes tunnel (default setting). The tunnel device need not be a cluster master, RF Domain manager, or VRRP master to establish the GRE tunnel. This is the default setting.</li><li>• cluster-master – Establishes tunnel only if the tunnel device is designated as the cluster master</li><li>• rf-domain-manager – Establishes tunnel only if the tunnel device is designated as the RF Domain manager</li><li>• vrrp-master &lt;1-255&gt; – Establishes tunnel only if the tunnel device is designated as the Virtual Router Redundancy (VRRP) master<ul style="list-style-type: none"><li>• &lt;1-255&gt; – Configures the VRRP group ID from 1 - 255. A VRRP group enables the creation of a group of routers as a default gateway for redundancy. Clients can point to the IP address of the VRRP virtual router as their default gateway and utilize a different group member if a master becomes unavailable.</li></ul></li></ul> |
|-------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Example

```
nx9500-6C8809(config-profile testNX9500-gre-tunnel-testGREtunnel)#establishment-criteria rf-domain-manager
```

```
nx9500-6C8809(config-profile testNX9500-gre-tunnel-testGREtunnel)#show context gre tunnel testGREtunnel establishment-criteria rf-domain-manager
```

```
nx9500-6C8809(config-profile testNX9500-gre-tunnel-testGREtunnel)#
```

failover

[gre-config-instance](#) on page 1003

Enables periodic pinging of the primary gateway to assess its availability. When enabled, the system continues pinging, an unreachable gateway, for a specified number of times and at the specified interval.

This option is disabled by default.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
failover interval <1-250> retry <1-10>
```

Parameters

```
failover interval <1-250> retry <1-10>
```

|                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>failover interval</b><br><b>&lt;1-250&gt; retry</b><br><b>&lt;1-10&gt;</b> | Specifies the interval, in seconds, between two successive pings to the primary gateway. If the primary gateway is unreachable, the system pings it at intervals specified here. <ul style="list-style-type: none"><li>• &lt;1-250&gt; - Specify a value from 1 - 250 seconds.</li><li>• retry - Specifies the maximum number attempts made to ping the primary gateway before the session is terminated.<ul style="list-style-type: none"><li>&lt;1-10&gt; - Specify a value from 1 - 10.</li></ul></li></ul> |
|-------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Example

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRE Tunnel)#failover interval 200 retry 5
```

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRE Tunnel)#show context gre tunnel testGRE Tunnel
dscp 20
failover interval 200 retry 5
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRE Tunnel)#
```

Related Commands

|                                 |                                                                |
|---------------------------------|----------------------------------------------------------------|
| <a href="#">no</a> on page 1008 | Removes the GRE tunnel settings based on the parameters passed |
|---------------------------------|----------------------------------------------------------------|

mtu

[gre-config-instance](#) on page 1003

Configures the MTU for IPv4/IPv6 L2GRE tunnel endpoints

The MTU is the largest physical packet size (in bytes) transmittable within the tunnel. Any messages larger than the configured MTU are divided into smaller packets before transmission. Larger the MTU greater is the efficiency because each packet carries more user data, while protocol overheads, such as headers or underlying per-packet delays remain fixed; the resulting higher efficiency means a slight improvement in bulk protocol throughput. A larger MTU results in the processing of fewer packets for the same amount of data.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000

- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
mtu [ipv4 <900-1476>|ipv6 <1236-1456>]
```

#### Parameters

```
mtu [ipv4 <900-1476>|ipv6 <1236-1456>]
```

|                                                           |                                                                                                                                                               |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mtu [ipv4 &lt;900-1476&gt; ipv6 &lt;1236-1456&gt;]</b> | Configures the MTU for L2GRE tunnel endpoints                                                                                                                 |
| <b>ipv4 &lt;900-1476&gt;</b>                              | <ul style="list-style-type: none"> <li>• ipv4 &lt;900-1476&gt; - Configures IPv4 L2GRE tunnel endpoint MTU from 900 - 1476. The default is 1476.</li> </ul>   |
| <b>ipv6 &lt;1236-1456&gt;</b>                             | <ul style="list-style-type: none"> <li>• ipv6 &lt;1236-1456&gt; - Configures IPv6 L2GRE tunnel endpoint MTU from 1236 - 1456. The default is 1456.</li> </ul> |

#### Example

```
nx9500-6C8809(config-profile testNX9500-gre-tunnel-testGREtunnel)#mtu ipv4 1200
```

```
nx9500-6C8809(config-profile testNX9500-gre-tunnel-testGREtunnel)#mtu ipv6 1300
```

```
nx9500-6C8809(config-profile testNX9500-gre-tunnel-testGREtunnel)#show context
gre tunnel testGREtunnel
 mtu ipv4 1200
 mtu ipv6 1300
 establishment-criteria rf-domain-manager
nx9500-6C8809(config-profile testNX9500-gre-tunnel-testGREtunnel)#
```

native

[gre-config-instance](#) on page 1003

Configures native trunking settings for this GRE tunnel

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
native [tagged|vlan <1-4094>]
```

#### Parameters

```
native [tagged|vlan <1-4094>]
```

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>native tagged</b>                        | <p>Enables native VLAN tagging</p> <p>The IEEE 802.1Q specification is supported for tagging frames and coordinating VLANs between devices. IEEE 802.1Q adds four bytes to each frame identifying the VLAN ID for upstream devices that the frame belongs to. If the upstream Ethernet device does not support IEEE 802.1Q tagging, it does not interpret the tagged frames. When VLAN tagging is required between devices, both devices must support tagging and be configured to accept tagged VLANs. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header so upstream Ethernet devices know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. This feature is disabled by default.</p> |
| <b>native vlan</b><br><b>&lt;1-4094&gt;</b> | <p>Specifies a numerical VLAN ID (1 - 4094) for the native VLAN</p> <p>The native VLAN allows an Ethernet device to associate untagged frames to a VLAN, when no 802.1q frame is included in the frame. Additionally, the native VLAN is the VLAN untagged traffic is directed over when using a port in trunk mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

### Example

```

nx9500-6C8809(config-profile testNX9500-gre-tunnel-testGREtunnel)#native tagged

nx9500-6C8809(config-profile testNX9500-gre-tunnel-testGREtunnel)#native vlan 20

nx9500-6C8809(config-profile testNX9500-gre-tunnel-testGREtunnel)#show context
gre tunnel testGREtunnel
 native vlan 20
 native tagged
 mtu ipv4 1200
 mtu ipv6 1300
 establishment-criteria rf-domain-manager
nx9500-6C8809(config-profile testNX9500-gre-tunnel-testGREtunnel)#

```

### Related Commands

|                        |                                                                |
|------------------------|----------------------------------------------------------------|
| <b>no</b> on page 1008 | Removes the GRE tunnel settings based on the parameters passed |
|------------------------|----------------------------------------------------------------|

no

[gre-config-instance](#) on page 1003

Removes or resets the GRE tunnel settings based on the parameters passed

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
no [dscp|establishment-criteria|failover|mtu|native|peer|tunneled-vlan]
```

```
no [dscp|establishment-criteria|failover|tunneled-vlan]
```

```
no mtu [ipv4|ipv6]
```

```
no native [tagged|vlan]
```

```
no peer <1-2>
```

Parameters

```
no <PARAMETERS>
```

|                                                                                                         |
|---------------------------------------------------------------------------------------------------------|
| <b>no &lt;PARAMETERS&gt;</b> Removes or resets the GRE tunnel's settings based on the parameters passed |
|---------------------------------------------------------------------------------------------------------|

Example

The following example shows the GRE tunnel 'testGREtunnel' settings before the no commands are executed:

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGREtunnel)#show context
gre tunnel testGREtunnel
 peer 1 ip 192.168.13.6
 native vlan 1
 tunneled-vlan 1,10
 native tagged
 dscp 20
 failover interval 200 retry 5
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGREtunnel)#
```

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGREtunnel)#no dscp
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGREtunnel)#no native vlan
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGREtunnel)#no tunneled-vlan
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGREtunnel)#no failover
```

The following example shows the GRE tunnel 'testGREtunnel' settings after the no commands are executed:

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGREtunnel)#show context
gre tunnel testGREtunnel
 peer 1 ip 192.168.13.6
 native tagged
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGREtunnel)#
```

peer

[gre-config-instance](#) on page 1003

Adds the GRE tunnel's end-point peers. A maximum of two peers, representing the tunnel's end points, can be added for each GRE tunnel.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
peer <1-2> ip <IPv4/IPv6>
```

Parameters

```
peer <1-2> ip <IPv4/IPv6>
```

|                                              |                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>peer &lt;1-2&gt; ip &lt;IPv4/IPv6&gt;</b> | <p>Configures the tunnel's end-point peers</p> <ul style="list-style-type: none"> <li>• &lt;1-2&gt; – Specify a numeric index for each peer to help differentiate the tunnel end points.</li> <li>• ip – Specify the IP address (IPv4/IPv6) of the added GRE peer to serve as a network address identifier.</li> </ul> <p>&lt;IPv4/IPv6&gt; – Specify the peer's IPv4 or IPv6 address.</p> |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Example

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGREtunnel)#peer 1 ip 192.168.13.6
```

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGREtunnel)#show context
gre tunnel testGREtunnel
 peer 1 ip 192.168.13.6
 native tagged
 dscp 20
 failover interval 200 retry 5
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGREtunnel)#
```

#### Related Commands

|                                 |                                                                |
|---------------------------------|----------------------------------------------------------------|
| <a href="#">no</a> on page 1008 | Removes the GRE tunnel settings based on the parameters passed |
|---------------------------------|----------------------------------------------------------------|

#### tunneled-vlan

[gre-config-instance](#) on page 1003

Defines the VLAN that connected clients use to route GRE tunneled traffic within their respective WLANs

Supported in the following platforms:

- Access Points – AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP8163, AP8432, AP8533
- Wireless Controllers – RFS4000
- Service Platforms – NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

**tunneled-vlan <VLAN-ID>**

#### Parameters

**tunneled-vlan <VLAN-ID>**

|                                      |                                                                                                                                                                                                                                                      |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>tunneled-vlan &lt;VLAN-ID&gt;</b> | <p>Specifies the VLANs associated with this GRE tunnel</p> <ul style="list-style-type: none"> <li>• &lt;VLAN-ID&gt; – Specify the VLAN IDs. Specify a comma-separated list of IDs, to specify multiple VLANs. For example, 1,10,12,16-20.</li> </ul> |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Example

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGREtunnel)# tunneled-vlan 10
```

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGREtunnel)#show context
gre tunnel testGREtunnel
 peer 1 ip 192.168.13.6
 native vlan 1
 tunneled-vlan 1,10
 native tagged
```

```
dscp 20
failover interval 200 retry 5
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRE Tunnel)#
```

#### Related Commands

|                                 |                                                                |
|---------------------------------|----------------------------------------------------------------|
| <a href="#">no</a> on page 1008 | Removes the GRE tunnel settings based on the parameters passed |
|---------------------------------|----------------------------------------------------------------|

### *http-analyze*

[Profile Config Commands](#) on page 862

Enables forwarding of HTTP request related data to the HTTP analytics engine

Wireless clients (MUs) connect to APs and route their HTTP requests through the APs. These APs extract and forward HTTP request packets, through MiNT, to the NX series controller. The NX series controller uses a new analytic daemon to cache, format, and forward information to the analytics engine. Currently the analytics daemon is supported only on the NX series service platform. Therefore, it is essential that all APs should use an NX series service platform as controller.

In a hierarchically organized network, HTTP analytics data forwarding is a simple and transparent process. The site controllers receive the HTTP data from adopted APs adopted. This data is compressed and forwarded to the Network Operations Center (NOC) controller. There is no need for a separate configuration to enable this feature.

Use this command to configure the mode and interval at which data is sent to the controller and the external analytics engine. This command also configures the external engine's details, such as URL, credentials, etc.

---

#### Note



The Analytics module helps gather data about customer behavior such as web sites visited, search terms used, mobile device types, number of new users vs. repeat users. This data provides a better understanding of pricing strategies and promotions being run by competitors.

---

#### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
http-analyze [compress|external-server|update-interval <1-3600>]
```

```
http-analyze [compress|update-interval <1-3600>
```

```
http-analyze external-server [password <WORD>|proxy <URL>|update-interval <1-3600>|url <URL>|username <WORD>|validate-server-certificate]
```

## Parameters

`http-analyze [compress|update-interval <1-3600>]`

|                                       |                                                                                                                                                                                                                                       |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>http-analyze</b>                   | Configures HTTP analysis related parameters                                                                                                                                                                                           |
| <b>compress</b>                       | Compresses update files before forwarding to the controller. This option is disabled by default.                                                                                                                                      |
| <b>update-interval &lt;1-3600&gt;</b> | Configures the interval, in seconds, at which buffered packets are pushed to the controller <ul style="list-style-type: none"><li>• &lt;1-3600&gt; - Specify the interval from 1 - 3600 seconds. The default is 60 seconds.</li></ul> |

`http-analyze external-server [password <WORD>|proxy <URL>|update-interval | url|username|validate-server-certificate]`

|                                       |                                                                                                                                                                                                                                                                                                              |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>http-analyze external-server</b>   | Configures the external HTTP analytics engine's parameters                                                                                                                                                                                                                                                   |
| <b>password &lt;WORD&gt;</b>          | Configures the external analytics engine's password <ul style="list-style-type: none"><li>• &lt;WORD&gt; - Provide the login password. This is the password associated with the user name needed to access the external analytics engine.</li></ul>                                                          |
| <b>proxy &lt;URL&gt;</b>              | Configures the proxy server's uniform resource locator (URL) <ul style="list-style-type: none"><li>• &lt;URL&gt; - Specify the proxy server's URL in the following format: <code>http://username:password@proxy-server:port</code>. For example, <code>http://mot:sym@wwwgate0.mot.com:1080</code></li></ul> |
| <b>update-interval &lt;1-3600&gt;</b> | Configures the interval, in seconds, at which buffered packets are pushed to the external analytics engine <ul style="list-style-type: none"><li>• &lt;1-3600&gt; - Specify the interval from 1 - 3600 seconds. The default is 60 seconds.</li></ul>                                                         |
| <b>url &lt;URL&gt;</b>                | Configures the external analytics engine's IP address or URL <ul style="list-style-type: none"><li>• &lt;URL&gt; - Provide the IP address or URL.</li></ul>                                                                                                                                                  |
| <b>username &lt;WORD&gt;</b>          | Configures the user name needed to access the external analytics engine <ul style="list-style-type: none"><li>• &lt;WORD&gt; - Provide the user name.</li></ul>                                                                                                                                              |
| <b>validate-server-certificate</b>    | Validates the external analytics engine's certificate, if it is using HTTPS as the mode of access                                                                                                                                                                                                            |

## Example

```
nx9500-6C8809(config-profile-default-rfs4000)#http-analyze compress

nx9500-6C8809(config-profile-default-rfs4000)#http-analyze update-interval 200

nx9500-6C8809(config-profile-default-rfs4000)#show context
profile rfs4000 default-rfs4000
 bridge vlan 1

 qos trust 802.1p
 interface pppoe1
 use firewall-policy default
 http-analyze update-interval 200
 http-analyze compress
 service pm sys-restart
 router ospf
```



```

nx9500-6C8809(config-profile-default-rfs4000)#

nx9500-6C8809(config-profile-test-nx5500)#http-analyze external-server username anonymous
nx9500-6C8809(config-profile-test-nx5500)#http-analyze external-server password anonymous
nx9500-6C8809(config-profile-test-nx5500)#http-analyze external-server validate-server-
certificate
nx9500-6C8809(config-profile-test-nx5500)#http-analyze external-server update-interval 100
nx9500-6C8809(config-profile-test-nx5500)#http-analyze external-server url
https://192.168.13.10

nx9500-6C8809(config-profile-test-nx5500)#show context
profile nx5500 test-nx5500
 no autoinstall configuration
 no autoinstall firmware

 interface ge5
 interface ge6
 interface pppoe1
 use firewall-policy default
 export startup-log max-retries 10 retry-interval 30 url ftp://
anonymous:anonymous@192.168.13.10/log/startup.log
 http-analyze external-server url https://192.168.13.10
 http-analyze external-server username anonymous
 http-analyze external-server password anonymous
 http-analyze external-server update-interval 100
 enforce-version adoption major
 enforce-version cluster full
 --More--
nx9500-6C8809(config-profile-test-nx5500)#

nx9500-6C8809(config-profile-test-nx5500)#http-analyze external-server proxy http://
mot:sym@wwwgate0.mot.com:1080

nx9500-6C8809(config-profile-test-nx5500)#show context
profile nx5500 test-nx5500
 no autoinstall configuration
 no autoinstall firmware
 crypto ikev1 policy ikev1-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default

 http-analyze external-server url https://192.168.13.10
 http-analyze external-server username anonymous
 http-analyze external-server password anonymous
 http-analyze external-server update-interval 100
 http-analyze external-server proxy http://mot:sym@wwwgate0.mot.com:1080
 enforce-version adoption major
 enforce-version cluster full
 service pm sys-restart
 router ospf
 router bgp
 dot1x system-auth-control
 dot1x use aaa-policy OnBoarding nx9500-6C8809(config-profile-test-nx5500)#

```

## Related Commands

|                                 |                                |
|---------------------------------|--------------------------------|
| <a href="#">no</a> on page 1200 | Disables HTTP analyze settings |
|---------------------------------|--------------------------------|

*interface*

[Profile Config Commands](#) on page 862

The following table summarizes interface configuration commands:

| Command                                                             | Description                                                                                                                   |
|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">interface</a> on page 1014                              | Selects an interface to configure                                                                                             |
| <a href="#">interface-config-ge-instance</a> on page 1017           | Summarizes Ethernet interface (associated with the wireless controller or service platform) configuration commands            |
| <a href="#">interface-config-vlan-instance</a> on page 1045         | Summarizes VLAN interface configuration commands                                                                              |
| <a href="#">interface-config-port-channel-instance</a> on page 1059 | Summarizes port-channel interface configuration commands                                                                      |
| <a href="#">interface-config-radio-instance</a> on page 1072        | Summarizes radio interface configuration commands (applicable to devices with built-in radios)                                |
| <a href="#">interface-config-wwan-instance</a> on page 1139         | Summarizes WWAN interface configuration commands                                                                              |
| <a href="#">interface-config-bluetooth-instance</a> on page 1146    | Summarizes the Bluetooth radio interface configuration commands (supported only on the AP8432 and AP8533 model access points) |

## interface

[interface](#) on page 1013

Selects an interface to configure

A profile's interface configuration can be defined to support separate physical Ethernet configurations both unique and specific to RFS4000 controllers and NX7500 and NX95XX series service platforms. Ports vary depending on the platform, but controller or service platform models do have some of the same physical interfaces.

A controller or service platform requires its virtual interface be configured for layer 3 (IP) access or layer 3 service on a VLAN. A virtual interface defines which IP address is associated with each VLAN ID the controller or service platform is connected to.

If the profile is configured to support an access point radio, an additional radio interface is available, unique to the access point's radio configuration.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax Service Platforms

```
interface [<INTERFACE-NAME>|fe <1-4>|ge <1-24>|me1|port-channel <1-4>|
pppoe1| radio [1|2|3]|serial <1-4>|tle1 <1-4>|up <1-2>|vlan <1-4094>|
wwan1|xge <1-4>]
```

Syntax Access Points and Wireless Controllers

```
interface [<INTERFACE-NAME>|bluetooth <1-1>|fe <1-4>|ge <1-8>|me1|port-
channel <1-4>|pppoe1|radio [1|2|3]|up1|vlan <1-4094>|wwan1|xge <1-4>]
```

#### Parameters

```
interface [<INTERFACE-NAME>|bluetooth <1-1>|fe <1-4>|ge <1-8>|me1|port-channel <1-4>|radio
[1|2|3]|serial <1-4>|tle1 <1-4>|up <1-2>|vlan <1-4094>|wwan1|xge <1-4>]
```

|                                 |                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;INTERFACE-NAME&gt;</b>   | Enters the configuration mode of the interface identified by the <INTERFACE-NAME> keyword                                                                                                                                                                                                                          |
| <b>bluetooth &lt;1-1&gt;</b>    | Selects the Bluetooth radio interface <ul style="list-style-type: none"> <li>• &lt;1-1&gt; - Specify the Bluetooth radio interface index from 1 - 1. As of now only one Bluetooth radio interface is supported.</li> </ul> <p>This interface is applicable only for the AP8432 and AP8533 model access points.</p> |
| <b>fe &lt;1-4&gt;</b>           | Selects a FastEthernet interface <ul style="list-style-type: none"> <li>• &lt;1-4&gt; - Specify the interface index from 1 - 4.</li> </ul>                                                                                                                                                                         |
| <b>ge &lt;1-24&gt;</b>          | Selects a GigabitEthernet interface <ul style="list-style-type: none"> <li>• &lt;1-24&gt; - Specify the interface index from 1 - 24. .</li> </ul>                                                                                                                                                                  |
| <b>me1</b>                      | Selects a management interface                                                                                                                                                                                                                                                                                     |
| <b>port-channel &lt;1-4&gt;</b> | Selects the port channel interface <ul style="list-style-type: none"> <li>• &lt;1-4&gt; - Specify the interface index from 1 - 4.</li> </ul>                                                                                                                                                                       |
| <b>pppoe1</b>                   | Selects the PPP over Ethernet interface to configure                                                                                                                                                                                                                                                               |
| <b>radio [1 2 3]</b>            | Selects a radio interface <ul style="list-style-type: none"> <li>• 1 - Selects radio interface 1</li> <li>• 2 - Selects radio interface 2</li> <li>• 3 - Selects radio interface 3</li> </ul> <p>The radio interface is not available on wireless controllers or service platforms.</p>                            |
| <b>up1</b>                      | Selects the uplink GigabitEthernet interface                                                                                                                                                                                                                                                                       |
| <b>vlan &lt;1-4094&gt;</b>      | Selects a VLAN interface <ul style="list-style-type: none"> <li>• &lt;1-4094&gt; - Specify the SVI VLAN ID from 1 - 4094.</li> </ul>                                                                                                                                                                               |
| <b>wwan1</b>                    | Selects a Wireless WAN interface<br>This interface is applicable only to AP7161, AP8163, RFS4000 model access points and controllers.                                                                                                                                                                              |
| <b>xge &lt;1-4&gt;</b>          | Selects a TenGigabitEthernet interface <ul style="list-style-type: none"> <li>• &lt;1-2&gt; - Specify the interface index from 1 - 4.</li> </ul>                                                                                                                                                                   |

#### Usage Guidelines

The ports available on a device vary depending on the model. For example, the following ports are available on RFS4000 and RFS7000 model wireless controllers:

- RFS4000 - ge1, ge2, ge3, ge4, ge5, up1
- GE ports on are RJ-45 supporting 10/100/1000Mbps

ME ports are out-of-band management ports used to manage the controller via CLI or Web UI, even when the other ports on the controller are unreachable.

The ports available on service platforms also vary depending on the model. For example, the following ports are available on NX series service platforms:

- NX7500 - ge1-ge10, xge1-xge2
- NX95XX series - ge1, ge2, xge1-xge4
- EX3500 - ge1-1 to ge1-24
- EX3548 - ge1-1 to ge1-48

GE ports are available on devices, such as RFS4000 controllers. GE ports are RJ-45 supporting 10/100/1000Mbps.

An UP port is used to connect to the backbone network. An UP port supports either RJ-45 or fiber. The UP port is the preferred means to connect to the backbone as it has a non-blocking 1gbps connection unlike the GE ports.

- The following ports are available on access points:
- AP6522 - GE1/POE (LAN)
- AP6562 - GE1/POE
- AP7161 - GE1/POE (LAN), GE2 (WAN)
- AP7502 - GE1 (THRU), fe1, fe2, fe3,
- AP7522 - GE1/POE (LAN)
- AP7532 - GE1/POE (LAN)
- AP8163 - GE1/POE (LAN), GE2 (WAN)



#### Note

For a NX7500 model service platform, there are options for either a 2 port or 4 port network management card. Either card can be managed using WiNG. If the 4 port card is used, ports ge7-ge10 are available. If the 2 port card is used, ports xge1-xge2 are available.

#### Example

```
nx9500-6C8809(config-profile-default-rfs4000-if-vlan44)#
nx9500-6C8809(config-profile-default-rfs4000-if-vlan44)#?
SVI configuration commands:
crypto Encryption module
description Vlan description
dhcp Dynamic Host Configuration Protocol (DHCP)
dhcp-relay-incoming Allow on-board DHCP server to respond to relayed DHCP
 packets on this interface
ip Interface Internet Protocol config commands
ipv6 Internet Protocol version 6 (IPv6)
no Negate a command or set its defaults
shutdown Shutdown the selected interface
use Set setting to use

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

nx9500-6C8809(config-profile-default-rfs4000-if-vlan44)#
```

## Related Commands

|                              |                                |
|------------------------------|--------------------------------|
| <code>no</code> on page 1200 | Removes the selected interface |
|------------------------------|--------------------------------|

### Interface-config-ge-instance

`interface` on page 1013

This section documents the GigabitEthernet configuration commands.

GE port placement and quantity varies depending on the controller, service platform, or access point model. Configure the GE interface either in the device's profile-config context or directly on a device.

The following example uses the config-profile-nx9500-6C8809 instance to configure a GigabitEthernet interface:

```
nx9500-6C8809(config-profile-testNX9000-if-ge2)#?
Interface configuration commands:
 captive-portal-enforcement Enable captive-portal enforcement on this port
 cdp Cisco Discovery Protocol
 channel-group Channel group commands
 description Interface specific description
 dot1x 802.1X
 duplex Set duplex to interface
 ip Internet Protocol (IP)
 ipv6 Internet Protocol version 6 (IPv6)
 lacp LACP commands
 lacp-channel-group LACP channel commands
 lldp Link Local Discovery Protocol
 mac-auth Enable mac-auth for this port
 no Negate a command or set its defaults
 power PoE Command
 qos Quality of service
 remove-override Remove configuration item override from the
 device (so profile value takes effect)
 shutdown Shutdown the selected interface
 spanning-tree Spanning tree commands
 speed Configure speed
 switchport Set switching mode characteristics
 use Set setting to use

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or
 terminal
```

```
nx9500-6C8809(config-profile-testNX9000-if-ge2)#
```

The following table summarizes the interface configuration commands:

| Command                                                 | Description                                                                                    |
|---------------------------------------------------------|------------------------------------------------------------------------------------------------|
| <a href="#">captive-portal-enforcement</a> on page 1018 | Enables captive-portal enforcement on this Ethernet port                                       |
| <a href="#">cdp</a> on page 1019                        | Enables Cisco Discovery Protocol (CDP) on this Ethernet port                                   |
| <a href="#">channel-group</a> on page 1020              | Assigns this Ethernet port to a channel group                                                  |
| <a href="#">description</a> on page 1021                | Configures a description for this Ethernet port                                                |
| <a href="#">dot1x (authenticator)</a> on page 1021      | Configures 802.1X authenticator settings                                                       |
| <a href="#">dot1x (supplicant)</a> on page 1024         | Configures 802.1X supplicant settings                                                          |
| <a href="#">duplex</a> on page 1025                     | Specifies the duplex mode for the interface                                                    |
| <a href="#">ip</a> on page 1026                         | Sets the IP address for this Ethernet port                                                     |
| <a href="#">ipv6</a> on page 1027                       | Sets the DHCPv6 and ICMPv6 neighbor discovery (ND) components for this interface               |
| <a href="#">lACP</a> on page 1029                       | Configures the selected GE port's Link Aggregation Control Protocol (LACP) port-priority value |
| <a href="#">lACP-channel-group</a> on page 1029         | Configures the selected GE port as a member of a port-channel group (also referred as LAG)     |
| <a href="#">lldp</a> on page 1031                       | Configures Link Local Discovery Protocol (LLDP)                                                |
| <a href="#">mac-auth</a> on page 1032                   | Enables MAC-based authentication on this Ethernet port                                         |
| <a href="#">no</a> on page 1033                         | Removes or reverts the selected Ethernet port settings                                         |
| <a href="#">power</a> on page 1034                      | Configures Power over Ethernet (PoE) settings on this interface                                |
| <a href="#">qos</a> on page 1035                        | Enables QoS                                                                                    |
| <a href="#">shutdown</a> on page 1036                   | Disables the selected Ethernet port                                                            |
| <a href="#">spanning-tree</a> on page 1036              | Configures spanning tree parameters                                                            |
| <a href="#">speed</a> on page 1038                      | Specifies the speed on this Ethernet port                                                      |
| <a href="#">switchport</a> on page 1039                 | Sets interface switching mode characteristics                                                  |
| <a href="#">use</a> on page 1043                        | Associates IPv4, IPv6, and/or MAC ACL with the selected Ethernet port                          |

## captive-portal-enforcement

[interface-config-ge-instance](#) on page 1017

Enables application of captive portal access permission rules to data transmitted over this specific Ethernet port. This setting is disabled by default.

Captive portal enforcement allows users on the wired network to pass traffic through the captive portal without being redirected to an authentication page. Authentication instead takes place when the

RADIUS server is queried against the wired user's MAC address. If the MAC address is in the RADIUS server's user database, the user can pass traffic on the captive portal.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
captive-portal-enforcement {fall-back}
```

Parameters

```
captive-portal-enforcement {fall-back}
```

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>captive-portal-enforcement fall-back</b> | Enables captive-portal enforcement on this Ethernet port <ul style="list-style-type: none"><li>• fall-back – Optional. Enforces captive portal validation only if port authentication fails. When selected, captive portal policies are enforced only when RADIUS authentication of the client MAC address is not successful. If this option is not selected, captive portal policies are enforced regardless of the client's MAC address being in the RADIUS server's user database or not.</li></ul> |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Example

```
nx9500-6C8809(config-device-B4-C7-99-6D-CD-4B-if-ge2)#captive-portal-enforcement
```

```
nx9500-6C8809(config-device-B4-C7-99-6D-CD-4B-if-ge2)#show context
interface ge2
captive-portal-enforcement
nx9500-6C8809(config-device-B4-C7-99-6D-CD-4B-if-ge2)#
```

Related Commands

|                                 |                                                       |
|---------------------------------|-------------------------------------------------------|
| <a href="#">no</a> on page 1033 | Disables captive-portal enforcement on this interface |
|---------------------------------|-------------------------------------------------------|

cdp

[interface-config-ge-instance](#) on page 1017

Enables CDP on the selected GE port

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
cdp [receive|transmit]
```

Parameters

```
cdp [receive|transmit]
```

|                 |                                                                                                                                                                                                                  |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>receive</b>  | Enables CDP packet snooping on this interface. When enabled, the port receives periodic interface updates from a multicast address. This option is enabled by default.                                           |
| <b>transmit</b> | Enables CDP packet transmission on this interface. When enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors. This option is enabled by default. |

#### Example

```
nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#cdp transmit
```

#### Related Commands

|                        |                                                                                        |
|------------------------|----------------------------------------------------------------------------------------|
| <b>no</b> on page 1033 | Disables CDP packet snooping on the controller or service platform's selected GE ports |
|------------------------|----------------------------------------------------------------------------------------|

### channel-group

[interface-config-ge-instance](#) on page 1017

Assigns this Ethernet port to a channel group. Ethernet ports can be aggregated to form a channel group. For example, an RFS7000 has four (4) Ethernet ports (1, 2, 3, & 4). These can be aggregated to form a minimum of one and maximum of two channel groups. A port can be a member of only one channel group at a time.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
channel-group <1-4>
```

#### Parameters

```
channel-group <1-4>
```

|                    |                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;1-4&gt;</b> | <p>Specifies a channel group number from 1 - 4. The number of channel groups supported varies with the device type. For example:</p> <ul style="list-style-type: none"> <li>• NX5500 - Supports three channel groups</li> <li>• NX75XX - Supports four channel groups</li> <li>• NX95XX - Supports two channel groups</li> </ul> <p><b>Note:</b> RFS4000 - Supports three channel groups.</p> |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Example

```
nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#channel-group 1
```

```
nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#show context
interface ge1
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
 channel-group 1
nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#
```

#### Related Commands



`no` on page 1033      Removes the channel group to which this port belongs

description

[interface-config-ge-instance](#) on page 1017

Configures a description for this Ethernet port

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

`description [ <LINE> | <WORD> ]`

Parameters

`description [ <LINE> | <WORD> ]`

|                     |                                                                                                                                     |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;LINE&gt;</b> | Configures the maximum length (number of characters) of the interface description                                                   |
| <b>&lt;WORD&gt;</b> | Configures a unique description for this interface. The description should not exceed the length specified by the <LINE> parameter. |

Example

```
nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#description "This is GigabitEthernet interface for Royal King"
```

```
nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#show context
interface ge1
 description "This is GigabitEthernet interface for Royal King"
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
 channel-group 1
nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#
```

Related Commands

`no` on page 1033      Removes the interface description

dot1x (authenticator)

[interface-config-ge-instance](#) on page 1017

Configures 802.1X authenticator settings

Dot1x (or 802.1x) is an IEEE standard for network authentication. It enables media-level (layer 2) access control, providing the capability to permit or deny connectivity based on user or device identity. Dot1x allows port-based access using authentication. An dot1x enabled port can be dynamically enabled or disabled depending on user identity or device connection.

Devices supporting dot1x allow the automatic provision and connection to the wireless network without launching a Web browser at login. When within range of a dot1x network, a device automatically connects and authenticates without needing to manually login.

Before authentication, the endpoint is unknown, and traffic is blocked. Upon authentication, the endpoint is known and traffic is allowed. The controller or service platform uses source MAC filtering to ensure only the authenticated endpoint is allowed to send traffic.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP8163, AP8432
- Wireless Controllers — RFS4000, NX5500, NX7500

Syntax

```
dot1x authenticator [guest-vlan | host-mode | max-reauth-req | port-control |
reauthenticate | timeout]
```

```
dot1x authenticator [guest-vlan <1-4094> | host-mode [multi-host | single-
host] | max-reauth-req <1-10> | port-control [auto | force-authorized | force-
unauthorized] | reauthenticate | timeout [quiet-period | reauth-period]
<1-65535>]
```



#### Note

The dot1x (802.1x) supplicant settings are documented in the next section.

Parameters

```
dot1x authenticator [guest-vlan <1-4094> | host-mode [multi-host | single-host] | max-reauth-
req <1-10> | port-control [auto | force-authorized | force-unauthorized] | reauthenticate | timeout
[quiet-period | reauth-period]]
```

|                                                                    |                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>dot1x authenticator</b>                                         | Configures 802.1x authenticator settings                                                                                                                                                                                                                                                            |
| <b>guest-vlan &lt;1-4094&gt;</b>                                   | Configures the guest VLAN for this interface. This is the VLAN, traffic is bridged on if this port is unauthorized and the guest VLAN is globally enabled. Select the VLAN index from 1 - 4094.                                                                                                     |
| <b>host-mode [multi-host   single-host]</b>                        | Configures the host mode for this interface <ul style="list-style-type: none"> <li>• multi-host – Configures multiple host mode</li> <li>• single-host – Configures single host mode. This is the default setting.</li> </ul>                                                                       |
| <b>max-reauth-req &lt;1-10&gt;</b>                                 | Configures maximum number of re-authorization retries for the supplicant. This is the maximum number of re-authentication attempts made before this port is moved to unauthorized. <ul style="list-style-type: none"> <li>• &lt;1-10&gt; – Specify a value from 1 -10. The default is 2.</li> </ul> |
| <b>port-control [auto   force-authorized   force-unauthorized]</b> | Configures port control state <ul style="list-style-type: none"> <li>• auto – Configures auto port state</li> <li>• force-authorized – Configures authorized port state. This is the default setting.</li> <li>• force-unauthorized – Configures unauthorized port state</li> </ul>                 |

|                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>reauthenticate</b>                                                             | Enables re-authentication for this port. When enabled, clients are forced to re-authenticate on this port. The setting is disabled by default. Therefore, clients are not required to re-authenticate for connection over this port until this setting is enabled.                                                                                                                                                                                                                                                                                                                |
| <b>timeout</b><br><b>[quiet-period   reauth-period]</b><br><b>&lt;1-65535&gt;</b> | <p>Configures timeout settings for this interface</p> <ul style="list-style-type: none"> <li>quiet-period – Configures the quiet period timeout in seconds. This is the interval, in seconds, between successive client authentication attempts.</li> <li>reauth-period – Configures the time after which re-authentication is initiated</li> </ul> <p>The following option is common to ‘quiet-period’ and ‘reauth-period’ keywords:</p> <ul style="list-style-type: none"> <li>&lt;1-65535&gt; – Specify a ‘quiet-period’ or ‘reauth-period’ from 1 - 65535 seconds.</li> </ul> |

### Example

```
rfs4000-229D58(config-profile-testRFS4000-if-gel)#dot1x authenticator guest-vlan 2

rfs4000-229D58(config-profile-testRFS4000-if-gel)#dot1x authenticator host-mode multi-host

rfs4000-229D58(config-profile-testRFS4000-if-gel)#dot1x authenticator max-reauth-req 6

rfs4000-229D58(config-profile-testRFS4000-if-gel)#dot1x authenticator reauthenticate

rfs4000-229D58(config-profile-testRFS4000-if-gel)#show context
interface gel
 dot1x authenticator host-mode multi-host
 dot1x authenticator guest-vlan 2
 dot1x authenticator reauthenticate
 dot1x authenticator max-reauth-count 6
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
rfs4000-229D58(config-profile-testRFS4000-if-gel)#
```

The following examples show the configurations made on an RFS4000 to enable it as a dot1X authenticator:

- 1 Configure AAA policy on the authenticator, and identify the authentication server as onboard (self):

```
rfs4000-229D58(config-aaa-policy-aaa-wireddot1x)#show context
aaa-policy aaa-wireddot1x
authentication server 1 onboard controller
rfs4000-229D58(config-aaa-policy-aaa-wireddot1x)#
```

This AAA policy is used in the authenticator’s self configuration mode as shown in the last step.

- 2 Configure RADIUS user policy on the authenticator:

```
rfs4000-229D58(config-radius-user-pool-wired-dot1x-users)#show con
radius-user-pool-policy wired-dot1x-users
user bob password 0 bob1234
rfs4000-229D58(config-radius-user-pool-wired-dot1x-users)#
```

The user name and password configured here should match that of the supplicant. For more information, see the examples provided in the [dot1x \(supplicant\)](#) on page 1024 section.

- 3 Configure RADIUS server policy on the authenticator, and associate the RADIUS user policy created in the previous step:

```
rfs4000-229D58(config-radius-server-policy-for-wired-dot1x)#show con
radius-server-policy for-wired-dot1x
use radius-user-pool-policy wired-dot1x-users
rfs4000-229D58(config-radius-server-policy-for-wired-dot1x)#
```

- 4 In the authenticator's self configuration mode, associate the RADIUS server policy, created in the previous step, and configure other parameters (in bold) as shown in the following example:  

```
rfs4000-229D58(config-device-00-15-70-81-73-79)#use radius-server-policy for-wired-dot1x
```
- 5 In the authenticator's interface > ge configuration mode, configure the following parameters:  

```
rfs4000-229D58(config-device-00-15-70-81-73-79-if-ge2)#dot1x authenticator host-mode single-host
rfs6000-817379(config-device-00-15-70-81-73-79-if-ge2)#dot1x authenticator port-control auto
```
- 6 In the authenticator's self configuration mode, configure the following parameters:  

```
rfs4000-229D58(config-device-00-15-70-81-73-79)#dot1x system-auth-control
rfs4000-229D58(config-device-00-15-70-81-73-79)#dot1x use aaa-policy aaa-wireddot1x
```

Following example displays the above configured parameters:

```
rfs4000-229D58(config-device-00-15-70-81-73-79)#show context
use profile default-rfs4000
use rf-domain default
hostname rfs4000-229D58
 use radius-server-policy for-wired-dot1x
interface mel
 ip address 192.168.0.1/24
interface ge2
 dot1x authenticator host-mode single-host
 dot1x authenticator port-control auto
interface vlan1
 ip address dhcp
 ip dhcp client request options all
logging on
logging console debugging
dot1x system-auth-control
dot1x use aaa-policy aaa-wireddot1x
--More--
rfs4000-229D58(config-device-00-15-70-81-73-79)#
```

#### Related Commands

|                                 |                                                         |
|---------------------------------|---------------------------------------------------------|
| <a href="#">no</a> on page 1033 | Disables or reverts interface settings to their default |
|---------------------------------|---------------------------------------------------------|

#### dot1x (supplicant)

[interface-config-ge-instance](#) on page 1017

Configures 802.1X supplicant (client) settings

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000, NX5500, NX7500

#### Syntax

```
dot1x supplicant username <USERNAME> password [0 <WORD>|2 <WORD>|<WORD>]
```

#### Parameters

```
dot1x supplicant username <USERNAME> password [0 <WORD>|2 <WORD>|<WORD>]
```

|                                                                              |                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>dot1x<br/>supplicant</b>                                                  | Configures 802.1x supplicant settings                                                                                                                                                                                                                                                                        |
| <b>username<br/>&lt;USERNAME&gt;</b>                                         | Sets the username for authentication <ul style="list-style-type: none"> <li>• &lt;USERNAME&gt; - Specify the supplicant's username.</li> </ul>                                                                                                                                                               |
| <b>password [0<br/>&lt;WORD&gt;   2<br/>&lt;WORD&gt;  <br/>&lt;WORD&gt;]</b> | Sets the password associated with the supplicant's username. Select any one of the following options: <ul style="list-style-type: none"> <li>• 0 &lt;WORD&gt; - Sets a clear text password</li> <li>• 2 &lt;WORD&gt; - Sets an encrypted password</li> <li>• &lt;WORD&gt; - Specify the password.</li> </ul> |

### Example

```
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#dot1x supplicant username bob
password 0 test@123
```

```
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#show context
interface ge1
 dot1x supplicant username bob password 0 test@123
 dot1x authenticator host-mode multi-host
 dot1x authenticator guest-vlan 2
 dot1x authenticator reauthenticate
 dot1x authenticator max-reauth-count 6
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#
```

The following example shows the configuration made on an AP7522 to enable it as a dot1X supplicant:

```
ap7522-85B19C(config-device-84-24-8D-85-B1-9C-if-ge2)#dot1x supplicant username bob
password 0 bob1234
ap7522-85B19C(config-device-84-24-8D-85-B1-9C)#show context
use profile default-ap7522
use rf-domain default
hostname ap7522-85B19C
no adoption-mode
interface ge1
 switchport mode access
 switchport access vlan 1
 dot1x supplicant username bob password 0 bob1234
logging on
logging console debugging
--More--
ap7522-85B19C(config-device-84-24-8D-85-B1-9C
```

### Related Commands

|                        |                                             |
|------------------------|---------------------------------------------|
| <b>no</b> on page 1033 | Removes 802.1X supplicant (client) settings |
|------------------------|---------------------------------------------|

### duplex

[interface-config-ge-instance](#) on page 1017

Configures duplex mode (for the flow of packets) on this Ethernet port

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

`duplex [auto|half|full]`

Parameters

`duplex [auto|half|full]`

|             |                                                                                                                                                                                                                                     |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>auto</b> | Enables automatic duplexity on an interface port. The port automatically detects whether it should run in full or half-duplex mode. (default setting)                                                                               |
| <b>half</b> | Sets the port to half-duplex mode. Allows communication in one direction only at any given time. When selected, data is sent over the port, then immediately data is received from the direction in which the data was transmitted. |
| <b>full</b> | Sets the port to full-duplex mode. Allows communication in both directions simultaneously. When selected, the port can send data while receiving data as well.                                                                      |

Example

```

nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#duplex full

nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#show context
interface ge1
 description "This is GigabitEthernet interface for Royal King"
 duplex full
 dot1x supplicant username Bob password 0 test@123
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
 channel-group 1
nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#

```

Related Commands

|                                 |                           |
|---------------------------------|---------------------------|
| <a href="#">no</a> on page 1033 | Reverts to default (auto) |
|---------------------------------|---------------------------|

ip

[interface-config-ge-instance](#) on page 1017

Sets the ARP and DHCP components for this Ethernet port

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

`ip [arp|dhcp]`

`ip [arp [header-mismatch-validation|trust]]|dhcp trust]`

Parameters

`ip [arp [header-mismatch-validation|trust]]|dhcp trust]`

|                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>arp [header-mismatch-validation trust]</b> | <p>Configures ARP packet settings</p> <ul style="list-style-type: none"> <li>header-mismatch-validation – Enables matching of source MAC address in the ARP and Ethernet headers to check for mismatch. This option is disabled by default.</li> <li>trust – Enables trust state for ARP responses on this interface. When enabled, ARP packets received on this port are considered trusted and information from these packets is used to identify rogue devices within the network. This option is disabled by default.</li> </ul> |
| <b>dhcp trust</b>                             | <p>Enables trust state for DHCP responses on this interface. When enabled, only DHCP responses are trusted and forwarded on this port, and a DHCP server can be connected only to a DHCP trusted port. This option is enabled by default.</p>                                                                                                                                                                                                                                                                                        |

#### Example

```

nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#ip dhcp trust

nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#ip arp header-mismatch-validation

rfs7000-37FABE(config-profile-default-rfs4000-if-ge1)#show context
interface ge1
description "This is GigabitEthernet interface for Royal King"
duplex full
dot1x supplicant username Bob password 0 test@123
ip dhcp trust
ip arp header-mismatch-validation
qos trust dscp
qos trust 802.1p
channel-group 1
nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#

```

#### Related Commands

|                                 |                                                                   |
|---------------------------------|-------------------------------------------------------------------|
| <a href="#">no</a> on page 1033 | Removes the ARP and DHCP components configured for this interface |
|---------------------------------|-------------------------------------------------------------------|

#### ipv6

[interface-config-ge-instance](#) on page 1017

Sets the DHCPv6 and ICMPv6 neighbor discovery (ND) components for this interface

The ICMPv6 ND protocol uses ICMP messages and solicited multicast addresses to track neighboring devices on the same local network. These messages are used to discover a neighbor's link layer address and to verify if a neighboring device is reachable.

The ICMP messages are neighbor solicitation (NS) and neighbor advertisement (NA) messages. When a destination host receives an NS message from a neighbor, it replies back with a NA. The NA contains the following information:

- Source address – This is the IPv6 address of the device sending the NA
- Destination address – This is the IPv6 address of the device from whom the NS message is received
- Data portion – Includes the link layer address of the device sending the NA

NS messages are used to verify a neighbor's (whose link layer address is known) reachability. To confirm a neighbor's reachability a node sends an NS message in which the neighbor's unicast address is specified as the destination address. If the neighbor sends back an acknowledgment on receipt of the NS message it is considered reachable.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
ipv6 [dhcpv6|nd]
```

```
ipv6 dhcpv6 trust
```

```
ipv6 nd [header-mismatch-validation|raguard|trust]
```

#### Parameters

```
ipv6 dhcpv6 trust
```

|                          |                                                                                                                                                                                                                                                  |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipv6 dhcpv6 trust</b> | Enables trust state for DHCPv6 responses on this interface. When enabled, all DHCPv6 responses received on this port are trusted and forwarded. This option is enabled by default.<br>A DHCPv6 server can be connected to a DHCPv6 trusted port. |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
ipv6 nd [header-mismatch-validation|raguard|trust]
```

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipv6 nd</b>                    | Configures IPv6 ND settings                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>header-mismatch-validation</b> | Enables matching of source MAC address in the ICMPv6 ND and Ethernet headers (link layer option) to check for mismatch. This option is disabled by default.                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>raguard</b>                    | Allows redirection of router advertisements (RAs) and ICMPv6 packets originating on this interface. When selected, RAs are periodically sent to hosts or sent in response to neighbor solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information. This option is enabled by default.                                                                                                                                                                                                                   |
| <b>trust</b>                      | Enables trust state for IPv6 ND requests received on this interface. When enabled, IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery protocol via ICMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to the request with a router advertisement packet containing Internet Layer configuration parameters. This option is disabled by default. |

#### Example

```
nx9500-6C8809(config-device-B4-C7-99-6D-CD-4B-if-gel)#ipv6 dhcpv6 trust
```

```
nx9500-6C8809(config-device-B4-C7-99-6D-CD-4B-if-gel)#ipv6 nd header-mismatch-validation
```

```
nx9500-6C8809(config-device-B4-C7-99-6D-CD-4B-if-gel)#ipv6 nd trust
```

```
nx9500-6C8809(config-device-B4-C7-99-6D-CD-4B-if-gel)#show context
```

```
interface gel
```

```
 switchport mode access
```

```
 switchport access vlan 1
```

```
 ipv6 nd trust
```

```
 ipv6 nd header-mismatch-validation
```

```
 ipv6 dhcpv6 trust
```

```
nx9500-6C8809(config-device-B4-C7-99-6D-CD-4B-if-gel)#
```

#### Related Commands



`no` on page 1033 Removes or reverts IPv6 settings on this interface

lACP

[interface-config-ge-instance](#) on page 1017

Configures the selected GE port's Link Aggregation Control Protocol (LACP) port-priority value. If LACP is enabled, and the selected port is a member of a link aggregation group (LAG), use this command to configure the port's priority within the LAG.

As per the IEEE 802.3ad standard, LACP enables aggregation of multiple physical links to form a single logical channel. Each aggregated group of physical links is a LAG. When enabled, LACP dynamically determines if link aggregation is possible between two peers, and automatically configures the aggregation. LACP also allows the switch to dynamically reconfigure the LAGs. The LAG is enabled only when LACP detects that the remote device is also using LACP and is able to join the LAG.

Enabling LACP provides automatic recovery in case one or more of the aggregated physical links fail.



#### Note

Use the [lACP-channel-group](#) on page 1029 command to configure this port as a LAG member.

Supported in the following platforms:

- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
lACP port-priority <1-65535>
```

Parameters

```
lACP port-priority <1-65535>
```

**lACP port-priority <1-65535>**

Configures the selected GE port's port-priority value. The selected port's actual priority within the LAG is determined by the port-priority value specified here along with the port's number. Higher the value, lower is the priority. Use this option to manipulate a port's priority. For example, in a LAG having five physical ports, four active and one standby, manually increasing the standby port's priority ensures that if one of the active port fails, the standby port is included in the LAG during re-negotiation.

- <1-65535> - Specify a value from 1 - 65535. The default value is 32768.

Example

```
nx9500-6C8809(config-profile-testnx9000-if-ge1)#lACP port-priority 2
```

```
nx9500-6C8809(config-profile-testnx9000-if-ge1)#show context
 interface ge1
 lACP port-priority 2
nx9500-6C8809(config-profile-testnx9000-if-ge1)#
```

Related Commands

`no` on page 1033 Removes the selected GE port's configured port-priority value

lACP-channel-group

[interface-config-ge-instance](#) on page 1017

Configures the selected GE port as a member of a port channel group (also referred as LAG)

As per the IEEE 802.3ad standard, LACP enables the aggregation of multiple physical links (ethernet ports) to form a single logical channel. When enabled, LACP dynamically determines if link aggregation is possible and then automatically configures the aggregation. LACP also allows the switch to dynamically reconfigure the LAGs. The LAG is enabled only when LACP detects that the remote device is also using LACP and is able to join the LAG.

#### Note



Successful aggregation of two or more physical links is feasible only if the aggregating physical links are configured identically. To ensure uniformity in configuration across LAG members, implement configuration changes (such as changes in the switching mode, speed, etc.) on the logical port (the port-channel) and not on the physical port. Changes made on the port-channel will cascade down to each member of the LAG thereby retaining uniformity.

Supported in the following platforms:

- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
lACP-channel-group <1-4> mode [active|passive]
```

#### Parameters

```
lACP-channel-group <1-4> mode [active|passive]
```

|                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>lACP-channel-group &lt;1-4&gt;</b> | <p>Associates this GE port with an existing port-channel group</p> <ul style="list-style-type: none"><li>• &lt;1-4&gt; – Specify a value from 1 - 4.</li></ul> <p>Use the interface &gt; port-channel &gt; &lt;1-4&gt; command to configure a port-channel group. For more information, see <a href="#">interface-config-port-channel-instance</a> on page 1059.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>mode [active passive]</b>          | <p>After configuring the selected port as a LAG member, specify whether the port is an active or passive member within the group. An active member initiates and participates in LACP negotiations.</p> <ul style="list-style-type: none"><li>• active – Configures the port as an active member. When set to active, the port always transmits LACPDU irrespective of the remote device's port mode.</li><li>• passive – Configures the port as passive member. When set to passive, the port will only respond to LACPDU received from its corresponding Active port.</li></ul> <p>At least one port within a LAG, on either of the two negotiating peers, should be in the active mode. LACP negotiations are not initiated if all LAG member ports are passive. Further, the peer-to-peer LACP negotiations are always initiated by the peer with the lower system-priority value. For more information on configuring the system-priority, see <a href="#">lACP</a> on page 1265.</p> |

#### Example

```
nx9500-6C8809(config-profile-testnx9000-if-ge1)#lACP-channel-group 2 mode active
```

```
nx9500-6C8809(config-profile-test2nx9000-if-ge1)#show context
interface ge1
 lACP-channel-group 2 mode active
 lACP port-priority 2
nx9500-6C8809(config-profile-test2nx900-if-ge1)#
```

To enable dynamic link aggregation on a device (service platform), execute the following steps:

- 1 Create a port-channel group on the device. Enter the port-channel configuration mode.

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#interface port-channel 1
```

Set the switching mode to access or trunk as per requirement. In this example, the mode is set to 'access'.

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09-if-port-channel1)#switchport mode access
```

Specify the VLAN to switch, commit changes and exit.

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09-if-port-channel1)#switchport access vlan 1
nx9500-6C8809(config-device-B4-C7-99-6C-88-09-if-port-channel1)#commit
nx9500-6C8809(config-device-B4-C7-99-6C-88-09-if-port-channel1)#exit
```

- 2 Enable dynamic link aggregation on the device's physical port. Enter the GE port's configuration mode.

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#interface ge 2
```

Enable link aggregation and associate the port with the port-channel group created in step 1.

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09-if-ge2)#lacp-channel-group 1 mode active
```

Note, the mode can be set to passive. However, at least one of the aggregated GE ports in the port-channel group should be active in order to initiate link aggregation negotiations with other LACP-enabled peers.

Specify the GE port's priority value.

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09-if-ge2)#lacp port-priority 2
```

#### Related Commands

|                                 |                                                              |
|---------------------------------|--------------------------------------------------------------|
| <a href="#">no</a> on page 1033 | Removes the selected GE port's port-channel group membership |
|---------------------------------|--------------------------------------------------------------|

#### lldp

[interface-config-ge-instance](#) on page 1017

Configures Link Local Discovery Protocol (LLDP) parameters on this Ethernet port

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
lldp [receive|transmit]
```

Parameters

```
lldp [receive|transmit]
```

|                 |                                                                                                                                                                                                       |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>receive</b>  | Enables LLDP Protocol Data Units (PDUs) snooping. When enabled, the port receives periodic updates from a multicast address informing about presence of neighbors. This option is enabled by default. |
| <b>transmit</b> | Enables LLDP PDU transmission. When enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors. This option is enabled by default.          |

#### Example

```
nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#lldp transmit
```

#### Related Commands

|                        |                                                         |
|------------------------|---------------------------------------------------------|
| <b>no</b> on page 1033 | Disables or reverts interface settings to their default |
|------------------------|---------------------------------------------------------|

## mac-auth

[interface-config-ge-instance](#) on page 1017

Enables authentication of MAC addresses on the selected wired port. When enabled, this feature authenticates the MAC address of a device, connecting to this interface, with a RADIUS server. When successfully authenticated, packets from the source are processed. Since only one MAC address is supported per wired port, packets from all other sources are dropped.

For more information on enabling this feature, see [mac-auth](#) on page 1183.

Enable port MAC authentication in conjunction with Wired 802.1x settings to configure a MAC authentication AAA policy.

This option is also available in the device configuration mode.

Supported in the following platforms:

- Access Points — AP6522 AP6562, AP7161, AP7502, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

**mac-auth**

#### Parameters

None

#### Example

```
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#mac-auth

rfs4000-229D58(config-profile-testRFS4000-if-ge1)#show context
interface ge1
 mac-auth
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
 channel-group 1
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#

rfs4000-229D58(config-profile-testRFS4000-if-ge5)#mac-auth
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-if-ge5)#show context
interface ge5
 switchport mode access
 switchport access vlan 1
 dot1x authenticator host-mode single-host
 dot1x authenticator guest-vlan 5
 dot1x authenticator port-control auto
 mac-auth
rfs4000-229D58(config-device-00-23-68-22-9D-58-if-ge5)#
```

#### Related Commands

|                                 |                                                                     |
|---------------------------------|---------------------------------------------------------------------|
| <a href="#">no</a> on page 1033 | Disables authentication of MAC addresses on the selected wired port |
|---------------------------------|---------------------------------------------------------------------|

no

[interface-config-ge-instance](#) on page 1017

Removes or reverts the selected Ethernet port settings

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
no [captive-portal-enforcement | cdp | channel-group | description | dot1x |
duplex | ip | ipv6 | lacp | lacp-channel-group | lldp | mac-auth | power | qos | shutdown |
spanning-tree | speed | switchport | use]
```

```
no [captive-portal-enforcement | channel-group | description | duplex | mac-auth |
shutdown | speed]
```

```
no [cdp | lldp] [receive | transmit]
```

```
no dot1x [authenticator [guest-vlan | host-mode | max-reauth-req | port-
control | reauthentication | timeout [quiet-period | reauth-period]] |
supplicant]
```

```
no ip [arp [header-mismatch-validation | trust] | dhcp trust]
```

```
no ipv6 [dhcpv6 trust | nd [header-mismatch-validation | rguard | trust]]
```

```
no [lacp port-priority | lacp-channel-group]
```

```
no power {best-effort | limit | priority}
```

```
no qos trust [802.1p | cos | dscp]
```

```
no spanning-tree [bpdufilter|bpduguard|force-version|guard|link-type|mst|portfast]
```

```
no switchport [access vlan|mode|trunk native tagged]
```

```
no use [ip-access-list|ipv6-access-list|mac-access-list] in
```

Parameters

```
no <PARAMETERS>
```

|                                                                                                            |
|------------------------------------------------------------------------------------------------------------|
| <b>no &lt;PARAMETERS&gt;</b> Removes or reverts this Ethernet port settings based on the parameters passed |
|------------------------------------------------------------------------------------------------------------|

Usage Guidelines

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#no cdp
```

```
nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#no duplex
power
```

[interface-config-ge-instance](#) on page 1017

Configures Power over Ethernet (PoE) settings on this interface

When configured, this option allows the selected port to use Power over Ethernet. When enabled, the controller supports 802.3af PoE on each of its GE ports. PoE allows users to monitor port power consumption and configure power usage limits and priorities for each GE port.

Supported in the following platforms:

- Wireless Controllers – RFS4000

Syntax

```
power {best-effort|limit <0-40>|priority [critical|high|low]}
```

Parameters

```
power {best-effort|limit <0-40>|priority [critical|high|low]}
```

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>power</b>                        | Configures power related thresholds for this interface                                                                                                                                                                                                                                                                                                                                               |
| <b>best-effort</b>                  | Optional. Enables power when the device is not operating from an 802.3at class 4 power source                                                                                                                                                                                                                                                                                                        |
| <b>limit &lt;0-40&gt;</b>           | Optional. Configures the PoE power limit from 0 - 40 Watts. The default is 30 Watts.                                                                                                                                                                                                                                                                                                                 |
| <b>priority [critical high low]</b> | Optional. Configures the PoE power priority on this interface. This is the priority assigned to this port versus the power requirements of the other ports available on the controller. <ul style="list-style-type: none"><li>• critical - Sets PoE priority as critical</li><li>• high - Sets PoE priority as high</li><li>• low - Sets PoE priority as low. This is the default setting.</li></ul> |

Example

```
rfs4000-229D58(config-profile-testRFS4000-if-ge1)#power limit 30
```

```

rfs4000-229D58(config-profile-testRFS4000-if-gel)#power priority critical

rfs4000-229D58(config-profile-testRFS4000-if-gel)#show context
interface gel
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
 power limit 30
 power priority critical
rfs4000-229D58(config-profile-testRFS4000-if-gel)#

```

#### Related Commands

|                                 |                                        |
|---------------------------------|----------------------------------------|
| <a href="#">no</a> on page 1033 | Removes PoE settings on this interface |
|---------------------------------|----------------------------------------|

#### qos

[interface-config-ge-instance](#) on page 1017

Defines Quality of Service (QoS) settings on this Ethernet port

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
qos trust [802.1p|cos|dscp]
```

#### Parameters

```
qos trust [802.1p|cos|dscp]
```

|                                |                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>trust [802.1p cos dscp]</b> | Trusts QoS values ingressing on this interface <ul style="list-style-type: none"> <li>• 802.1p - Trusts 802.1p COS values ingressing on this interface</li> <li>• cos - Trusts 802.1p COS values ingressing on this interface. This option is enabled by default.</li> <li>• dscp - Trusts IP DSCP QOS values ingressing on this interface. This option is enabled by default.</li> </ul> |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Example

```

nx9500-6C8809(config-profile-default-rfs4000-if-gel)#qos trust dscp

nx9500-6C8809(config-profile-default-rfs4000-if-gel)#qos trust 802.1p

nx9500-6C8809(config-profile-default-rfs4000-if-gel)#show context
interface gel
 description "This is GigabitEthernet interface for Royal King"
 duplex full
 dot1x supplicant username Bob password 0 test@123
 ip dhcp trust
 ip arp header-mismatch-validation
 qos trust dscp
 qos trust 802.1p
 channel-group 1
nx9500-6C8809(config-profile-default-rfs4000-if-gel)#

```

## Related Commands

|                                 |                                                |
|---------------------------------|------------------------------------------------|
| <a href="#">no</a> on page 1033 | Removes QoS settings on the selected interface |
|---------------------------------|------------------------------------------------|

## shutdown

[interface-config-ge-instance](#) on page 1017

Shuts down (disables) an interface. The interface is administratively enabled unless explicitly disabled using this command.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

**shutdown**

### Parameters

None

### Example

```
nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#shutdown
```

## Related Commands

|                                 |                                                         |
|---------------------------------|---------------------------------------------------------|
| <a href="#">no</a> on page 1033 | Disables or reverts interface settings to their default |
|---------------------------------|---------------------------------------------------------|

## spanning-tree

[interface-config-ge-instance](#) on page 1017

Configures spanning tree parameters

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
spanning-tree [bpdufilter|bpduguard|force-version|guard|link-type|mst|
port-cisco-interopability|portfast]
```

```
spanning-tree [force-version <0-3>|guard root|portfast]
```

```
spanning-tree [bpdufilter|bpduguard] [default|disable|enable]
```

```
spanning-tree link-type [point-to-point|shared]
```



```
spanning-tree mst <0-15> [cost <1-200000000>|port-priority <0-240>]
```

```
spanning-tree port-cisco-interoperability [disable|enable]
```

#### Parameters

```
spanning-tree [force-version <0-3>|guard root|portfast]
```

|                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>force-version</b><br><b>&lt;0-3&gt;</b> | Specifies the spanning tree force version. A version identifier of less than 2 enforces the spanning tree protocol. Select one of the following versions: <ul style="list-style-type: none"><li>• 0 - Spanning Tree Protocol (STP)</li><li>• 1 - Not supported</li><li>• 2 - Rapid Spanning tree Protocol (RSTP)</li><li>• 3 - Multiple Spanning Tree Protocol (MSTP). This is the default setting</li></ul>                                                                                                                           |
| <b>guard root</b>                          | Enables Root Guard for the port<br>The Root Guard disables superior Bridge Protocol Data Unit (BPDU) reception. The Root Guard ensures the enabled port is a designated port. If the Root Guard enabled port receives a superior BPDU, it moves to a discarding state (root-inconsistent STP state). This state is equivalent to a listening state, and data is not forwarded across the port. Therefore, enabling the guard root enforces the root bridge position. Use the no parameter with this command to disable the Root Guard. |
| <b>portfast</b>                            | Enables rapid transitions. Enabling PortFast allows the port to bypass the listening and learning states.                                                                                                                                                                                                                                                                                                                                                                                                                              |

```
spanning-tree [bpdupfilter|bpduguard] [default|disable|enable]
```

|                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>bpdupfilter</b><br><b>[default  </b><br><b>disable  </b><br><b>enable]</b> | Sets a PortFast BPDU filter for the port<br>Use the no parameter with this command to revert the port BPDU filter to its default.<br>The spanning tree protocol sends BPDUs from all ports. Enabling the BPDU filter ensures PortFast enabled ports do not transmit or receive BPDUs.                                                                                                                                                                                     |
| <b>bpduguard</b><br><b>[default  </b><br><b>disable  </b><br><b>enable]</b>   | Enables BPDU guard on a port<br>Use the no parameter with this command to set BPDU guard to its default.<br>When the BPDU guard is set for a bridge, all PortFast-enabled ports that have the BPDU guard set to default shut down upon receiving a BPDU. If this occurs, the BPDU is not processed. The port can be brought back either manually (using the no shutdown command), or by configuring the errdisable-timeout to enable the port after a specified interval. |

```
spanning-tree link-type [point-to-point|shared]
```

|                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>link-type</b><br><b>[point-to-</b><br><b>point  shared]</b> | Enables point-to-point or shared link types <ul style="list-style-type: none"><li>• point-to-point - Enables rapid transition. This option indicates the port should be treated as connected to a point-to-point link. A port connected to a controller is a point-to-point link.</li><li>• shared - Disables rapid transition. This option indicates this port should be treated as having a shared connection. A port connected to a hub is on a shared link,</li></ul> |
|----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
spanning-tree mst <0-15> [cost <1-200000000>|port-priority <0-240>]
```

|                                        |                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mst &lt;0-15&gt;</b>                | Configures MST on a spanning tree                                                                                                                                                                                                                                                                                                   |
| <b>cost<br/>&lt;1-200000000&gt;</b>    | Defines path cost for a port from 1 - 200000000. The default path cost depends on the speed of the port. The cost helps determine the role of the port in the MSTP network. The designated cost is the cost for a packet to travel from this port to the root in the MSTP configuration. The slower the media, the higher the cost. |
| <b>port-priority<br/>&lt;0-240&gt;</b> | Defines port priority for a bridge from 1 - 240. Lower the priority greater is the likelihood of the port becoming a designated port. Applying a higher value impacts the port's likelihood of becoming a designated port.                                                                                                          |

spanning-tree port-cisco-interoperability [disable|enable]

|                                    |                                                                                                  |
|------------------------------------|--------------------------------------------------------------------------------------------------|
| <b>port-cisco-interoperability</b> | Enables interoperability with Cisco's version of MSTP (which is incompatible with standard MSTP) |
| <b>enable</b>                      | Enables CISCO Interoperability                                                                   |
| <b>disable</b>                     | Disables CISCO Interoperability. The default is disabled.                                        |

#### Example

```

nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#spanning-tree bpdudfilter disable

nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#spanning-tree bpduguard enable

nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#spanning-tree force-version 1

nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#spanning-tree guard root

nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#spanning-tree mst 2 port-priority 10

nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#show context
interface ge1
 description "This is GigabitEthernet interface for Royal King"
 duplex full
 spanning-tree bpduguard enable
 spanning-tree bpdudfilter disable
 spanning-tree force-version 1
 spanning-tree guard root
 spanning-tree mst 2 port-priority 10
--More--
nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#

```

#### Related Commands

|                        |                                                             |
|------------------------|-------------------------------------------------------------|
| <b>no</b> on page 1033 | Removes spanning tree settings configured on this interface |
|------------------------|-------------------------------------------------------------|

speed

[interface-config-ge-instance](#) on page 1017

Specifies the speed of a FastEthernet (10/100) or GigabitEthernet (10/100/1000) port. This is the speed at which the port can receive and transmit the data.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000

- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

`speed [10|100|1000|auto]`

#### Parameters

`speed [10|100|1000|auto]`

|             |                                                                                                                                                                                                                                                                                                                                                                   |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>10</b>   | Forces 10 Mbps operation                                                                                                                                                                                                                                                                                                                                          |
| <b>100</b>  | Forces 100 Mbps operation                                                                                                                                                                                                                                                                                                                                         |
| <b>1000</b> | Forces 1000 Mbps operation                                                                                                                                                                                                                                                                                                                                        |
| <b>auto</b> | Port automatically detects its operational speed based on the port at the other end of the link. Select this option to enable the port to automatically exchange information about data transmission speed and duplex capabilities. Auto negotiation is helpful when in an environment where different devices are connected and disconnected on a regular basis. |

#### Usage Guidelines

Set the interface speed to auto detect and use the fastest speed available. Speed detection is based on connected network hardware.

#### Example

```
nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#speed 10

nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#show context
interface ge1
 description "This is GigabitEthernet interface for Royal King"
 speed 10
 duplex full
 spanning-tree bpduguard enable
 spanning-tree bpdufilter disable
 spanning-tree force-version 1
 spanning-tree guard root
 spanning-tree mst 2 port-priority 10
 dot1x supplicant username Bob password 0 test@123
 ip dhcp trust
 ip arp header-mismatch-validation
 qos trust dscp
 qos trust 802.1p
 channel-group 1
nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#
```

#### Related Commands

|                                 |                                |
|---------------------------------|--------------------------------|
| <a href="#">no</a> on page 1033 | Resets speed to default (auto) |
|---------------------------------|--------------------------------|

#### switchport

[interface-config-ge-instance](#) on page 1017

Sets switching mode characteristics for the selected interface

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
switchport [access|mode|trunk]
```

```
switchport access vlan [<1-4094>|<VLAN-ALIAS-NAME>]
```

```
switchport mode [access|trunk]
```

```
switchport trunk [allowed|fabric-attach|native]
```

```
switchport trunk allowed vlan [<VLAN-ID>|add <VLAN-ID>|none|remove <VLAN-ID>]
```

```
switchport trunk fabric-attach vlan [<1-4094>|<VLAN-ALIAS-NAME>] isid <1-16777214>
```

```
switchport trunk native [tagged|vlan [<1-4094>|<VLAN-ALIAS-NAME>]]
```

Parameters

```
switchport access vlan [<1-4094>|<VLAN-ALIAS-NAME>]
```

|                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>access vlan</b><br/>[&lt;1-4094&gt; &lt;VLAN-ALIAS-NAME&gt;]</p> | <p>Sets the VLAN when interface is in the access mode. You can either directly specify the native VLAN ID or use a VLAN alias to identify the native VLAN.</p> <ul style="list-style-type: none"> <li>• &lt;1-4094&gt; - Specify the SVI VLAN ID from 1 - 4094.</li> <li>• &lt;VLAN-ALIAS-NAME&gt; - Specify the VLAN alias name (should be existing and configured).</li> </ul> <p>An Ethernet port in the access mode accepts packets only from the native VLAN. Frames are forwarded out the port untagged with no 802.1Q header. All frames received on the port are expected as untagged and are mapped to the native VLAN.</p> |
|------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
switchport mode [access|trunk]
```

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>mode [access trunk]</b></p> | <p>Sets the interface's switching mode to access or trunk (can only be used on physical - layer 2 - interfaces)</p> <ul style="list-style-type: none"> <li>• access - If access mode is selected, the access VLAN is automatically set to VLAN1. In this mode, only untagged packets in the access VLAN (vlan1) are accepted on this port. All tagged packets are discarded.</li> <li>• trunk - If trunk mode is selected, tagged VLAN packets are accepted. The native VLAN is automatically set to VLAN1. Untagged packets are placed in the native VLAN by the wireless controller or service platform. Outgoing packets in the native VLAN are sent untagged. The default mode for both ports is trunk.</li> </ul> |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
switchport trunk allowed vlan [<VLAN-ID>|add <VLAN-ID>|none|remove <VLAN-ID>]
```

|                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>trunk allowed</b>                                                                | Sets trunking mode, allowed VLANs characteristics of the port. Use this option to add VLANs that exclusively send packets over the listed port.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>vlan [&lt;VLAN-ID&gt;   add &lt;VLAN-ID&gt;   none   remove &lt;VLAN-ID&gt;]</b> | <p>Sets allowed VLAN options. The options are:</p> <ul style="list-style-type: none"> <li>• &lt;VLAN-ID&gt; – Allows a group of VLAN IDs. Specify the VLAN IDs, can be either a range (55-60) or a comma-separated list (35, 41, etc.)</li> <li>• none – Allows no VLANs to transmit or receive through the layer 2 interface</li> <li>• add &lt;VLAN-ID&gt; – Adds VLANs to the current list <ul style="list-style-type: none"> <li>• &lt;VLAN-ID&gt; – Specify the VLAN IDs. Can be either a range of VLAN (55-60) or a list of comma separated IDs (35, 41, etc.)</li> </ul> </li> <li>• remove &lt;VLAN-ID&gt; – Removes VLANs from the current list <ul style="list-style-type: none"> <li>• &lt;VLAN-ID&gt; – Specify the VLAN IDs. Can be either a range of VLAN (55-60) or a list of comma separated IDs (35, 41, etc.)</li> </ul> </li> </ul> <p>Allowed VLANs are configured only when the switching mode is set to “trunk”.</p> |

```
switchport trunk fabric-attach vlan [<1-4094>|<VLAN-ALIAS-NAME>] isid <1-16777214>
```

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| trunk         | Sets trunking mode characteristics of this Ethernet port                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| fabric-attach | <p>Enables FA (Fabric Attach) client operation on this Ethernet port. Use this option to enable non-SPB WiNG devices (access points and controllers) as FA Clients. FA enabled switches, in the FC network, send out LLDP messages with TLV extensions of Organization-specific TLV with OUI, to discover FA clients and advertise capabilities.</p> <p>The FA-enabled client associates with the FA Server (FAS), and obtains provisioning information (management VLAN interface details, and whether the interface is tagged or not) that allows the client to be configured with parameters that allow traffic to flow through the Fabric to the WLAN controller. This initial FA Client to WLC communication uses the Fabric’s default VLAN to I-SID mapping. Use this command to configure the I-SID (Individual Service Identifier) to VLAN mapping that the FA Client uses to negotiate with the FAS.</p> <p><b>Note:</b> You can configure FA Client capability on a device’s profile as well as device contexts.</p> <p><b>Note:</b> This option is enabled only when the switching mode is set to trunk.</p> |

|                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>vlan [&lt;1-4094&gt; &lt;VLAN-ALIAS-NAME&gt;]</pre> | <p>Configures the VLAN through which traffic from this device is routed to the FA switch</p> <ul style="list-style-type: none"> <li>• &lt;1-4094&gt; - Specify the VLAN from 1 - 4094.</li> <li>• &lt;VLAN-ALIAS-NAME&gt; - Use a VLAN alias to specify the VLAN. If using a VLAN alias, ensure that the alias is existing and configured.</li> </ul> <p>The FA Client requests acceptance of the I-SID to VLAN mapping from the FAS within the FC (Fabric Connect) network. Once acceptance is achieved, the FC edge switch applies the I-SID to the VLAN traffic from the device (AP or controller), and uses this I-SID inside the Fabric.</p> <p><b>Note:</b> Both the FA Client and FA switch (at the edge of the FC network) use LLDP Element and Assignment Type-Length-Values (TLVs) to advertise their identity and FA capabilities.</p> |
| <pre>isid &lt;1-16777214&gt;</pre>                       | <p>Configures the I-SID to be associated with the VLAN interface specified above.</p> <ul style="list-style-type: none"> <li>• isid &lt;1-16777214&gt; - Specify the I-SID from 1 - 16777214. The IEEE Auto-Attach standard requires that the I-SID and VLAN ID be unique per port per switch, so that the device does not enforce duplicate I-SID and VLAN ID for each mapping.</li> </ul> <p><b>Note:</b> A maximum of 94 pairs of I-SID to VLAN mappings can be configured per Ethernet port.</p>                                                                                                                                                                                                                                                                                                                                              |

```
switchport trunk native [tagged|vlan [<1-4094>|<VLAN-ALIAS-NAME>]]
```

|                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre><b>trunk</b></pre>                                                         | <p>Sets trunking mode characteristics of the switchport</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <pre><b>native [tagged vlan [&lt;1-4094&gt; &lt;VLAN-ALIAS-NAME&gt;]]</b></pre> | <p>Configures the native VLAN ID for the trunk-mode port</p> <p>The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN untagged traffic is directed over when using a port in trunk mode.</p> <ul style="list-style-type: none"> <li>• tagged - Tags the native VLAN. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header enabling upstream Ethernet devices to know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. A native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame.</li> <li>• vlan [&lt;1-4094&gt; &lt;VLAN-ALIAS-NAME&gt;] - Sets the native VLAN for classifying untagged traffic when the interface is in trunking mode. <ul style="list-style-type: none"> <li>• &lt;1-4094&gt; - Specify a value from 1 - 4094.</li> <li>• &lt;VLAN-ALIAS-NAME&gt; - Specify the VLAN alias name used to identify the VLANs. The VLAN alias should be existing and configured.</li> </ul> </li> </ul> |

#### Usage Guidelines

Interfaces ge1 - ge4 can be configured as trunk or in access mode. An interface configured as “trunk” allows packets (from the given list of VLANs) to be added to the trunk. An interface configured as “access” allows packets only from native VLANs.

Use the [no] `switchport (access|mode|trunk)` to undo switchport configurations.

#### Example

```
nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#switchport trunk native tagged
```

```

nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#switchport access vlan 1

nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#show context
interface ge1
 description "This is GigabitEthernet interface for Royal King"
 speed 10
 duplex full
 switchport mode access
 switchport access vlan 1
 spanning-tree bpduguard enable
 spanning-tree bpdufilter disable
 --More--
nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#

```

The following is the basic configuration required to enable a device as a FA Client, with tagged native VLAN traffic:

```

ap8432-070235(config-device-74-67-F7-07-02-35-if-ge1)#switchport mode trunk
ap8432-070235(config-device-74-67-F7-07-02-35-if-ge1)#switchport trunk
fabric-attach vlan 1 isid 1
ap8432-070235(config-device-74-67-F7-07-02-35-if-ge1)#switchport trunk
fabric-attach vlan 2 isid 200
ap8432-070235(config-device-74-67-F7-07-02-35-if-ge1)#switchport trunk
fabric-attach vlan 100 isid 1000
ap8432-070235(config-device-74-67-F7-07-02-35-if-ge1)#switchport trunk
allowed vlan 1-2,100
ap8432-070235(config-device-74-67-F7-07-02-35-if-ge1)#switchport trunk
native tagged
ap8432-070235(config-device-74-67-F7-07-02-35-if-ge1)#show context
interface ge1
 switchport mode trunk
 switchport trunk fabric-attach vlan 1 isid 1
 switchport trunk fabric-attach vlan 2 isid 200
 switchport trunk fabric-attach vlan 100 isid 1000
 switchport trunk native vlan 1
 no switchport trunk native tagged
 switchport trunk allowed vlan 1-2,100
ap8432-070235(config-device-74-67-F7-07-02-35-if-ge1)#

```

#### Related Commands

|                                 |                                                         |
|---------------------------------|---------------------------------------------------------|
| <a href="#">no</a> on page 1033 | Disables or reverts interface settings to their default |
|---------------------------------|---------------------------------------------------------|

use

[interface-config-ge-instance](#) on page 1017

Specifies the IP (IPv4 and IPv6) access list and MAC access list used with this Ethernet port. The associated ACL firewall inspects IP and MAC traffic flows and detects attacks typically not visible to traditional wired firewall appliances.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
use [ip-access-list in <IPv4-ACCESS-LIST-NAME>|ipv6-access-list <IPv6-ACCESS-LIST-NAME>|mac-access-list in <MAC-ACCESS-LIST-NAME>]
```

#### Parameters

```
use [ip-access-list in <IPv4-ACCESS-LIST-NAME>|ipv6-access-list <IPv6-ACCESS-LIST-NAME>|mac-access-list in <MAC-ACCESS-LIST-NAME>]
```

|                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ip-access-list in &lt;IPv4-ACCESS-LIST-NAME&gt;</b>   | Associates an IPv4 access list with this Ethernet port. IPv4 is a connectionless protocol for packet switched networking. IPv4 operates as a best effort delivery method, as it does not guarantee delivery, and does not ensure proper sequencing or duplicate delivery (unlike (TCP). IPv4 hosts can use link local addressing to provide local connectivity. <ul style="list-style-type: none"><li>• in - Applies the IPv4 ACL on incoming packets<ul style="list-style-type: none"><li>• &lt;IPv4-ACCESS-LIST-NAME&gt; - Specify the IPv4 access list name (it should be an existing and configured).</li></ul></li></ul> |
| <b>ipv6-access-list in &lt;IPv6-ACCESS-LIST-NAME&gt;</b> | Associates an IPv6 access list with this Ethernet port. IPv6 is the latest revision of the IP designed to replace IPv4. IPv6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. <ul style="list-style-type: none"><li>• in - Applies the IPv6 ACL on incoming packets<ul style="list-style-type: none"><li>• &lt;IPv6-ACCESS-LIST-NAME&gt; - Specify the IPv6 access list name (it should be an existing and configured).</li></ul></li></ul>               |
| <b>mac-access-list in &lt;MAC-ACCESS-LIST-NAME&gt;</b>   | Associates a MAC access list with this Ethernet port. MAC ACLs filter/mark packets based on the MAC address from which they arrive, as opposed to filtering packets on layer 2 ports. <ul style="list-style-type: none"><li>• in - Applies the MAC ACL on incoming packets<ul style="list-style-type: none"><li>• &lt;MAC-ACCESS-LIST-NAME&gt; - Specify the MAC access list name (it should be an existing and configured).</li></ul></li></ul>                                                                                                                                                                              |

#### Example

```
nx9500-6C8809(config-profile-default-rfs4000-if-gel)#use mac-access-list in test

nx9500-6C8809(config-profile-default-rfs4000-if-gel)#use ip-access-list in test

nx9500-6C8809(config-profile-default-rfs4000-if-gel)#show context
interface gel
description "This is GigabitEthernet interface for Royal King"
speed 10
duplex full
switchport mode accessi
switchport access vlan 1
use ip-access-list in test
use mac-access-list in test
spanning-tree bpduguard enable
spanning-tree bpdufilter disable
spanning-tree force-version 1
--More--
nx9500-6C8809(config-profile-default-rfs4000-if-gel)#
```

#### Related Commands

|                        |                                                                        |
|------------------------|------------------------------------------------------------------------|
| <b>no</b> on page 1033 | Disassociates the IP access list or MAC access list from the interface |
|------------------------|------------------------------------------------------------------------|



## interface-config-vlan-instance

[interface](#) on page 1013

Use the config-profile-<DEVICE-PROFILE-NAME> mode to configure Ethernet, VLAN and tunnel settings.

To switch to this mode, use the following commands:

```
<DEVICE>(config-profile-default-<DEVICE-TYPE>)#interface [<INTERFACE-NAME>| fe <1-4>|ge <1-24>|me1|port-channel <1-4>|pppoe1|radio [1|2|3]|up1|vlan <1-4094>| wwan1|xge <1-24>]
```

The following example uses the config-profile-nx9500-6C8809 instance to configure a VLAN interface:

```
nx9500-6C8809(config-profile-default-rfs4000)#interface vlan 8
nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#
```

```
nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#?
```

SVI configuration commands:

|                     |                                                                                 |
|---------------------|---------------------------------------------------------------------------------|
| crypto              | Encryption module                                                               |
| description         | Vlan description                                                                |
| dhcp                | Dynamic Host Configuration Protocol (DHCP)                                      |
| dhcp-relay-incoming | Allow on-board DHCP server to respond to relayed DHCP packets on this interface |
| ip                  | Interface Internet Protocol config commands                                     |
| ipv6                | Internet Protocol version 6 (IPv6)                                              |
| no                  | Negate a command or set its defaults                                            |
| shutdown            | Shutdown the selected interface                                                 |
| use                 | Set setting to use                                                              |
| clrscr              | Clears the display screen                                                       |
| commit              | Commit all changes made in this session                                         |
| do                  | Run commands from Exec mode                                                     |
| end                 | End current mode and change to EXEC mode                                        |
| exit                | End current mode and down to previous mode                                      |
| help                | Description of the interactive help system                                      |
| revert              | Revert changes                                                                  |
| service             | Service Commands                                                                |
| show                | Show running system information                                                 |
| write               | Write running configuration to memory or terminal                               |

```
nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#
```

The following table summarizes interface VLAN configuration commands:

| Commands                                         | Description                                                                        |
|--------------------------------------------------|------------------------------------------------------------------------------------|
| <a href="#">crypto</a> on page 1046              | Defines the encryption module used with this VLAN interface                        |
| <a href="#">description</a> on page 1046         | Defines the VLAN interface description                                             |
| <a href="#">dhcp</a> on page 1047                | Enables inclusion of optional fields (client identifier) in DHCP client requests   |
| <a href="#">dhcp-relay-incoming</a> on page 1048 | Allows an onboard DHCP server to respond to relayed DHCP packets on this interface |
| <a href="#">ip</a> on page 1048                  | Configures the VLAN interface's IP settings                                        |
| <a href="#">ipv6</a> on page 1051                | Configures the VLAN interface's IPv6 settings                                      |
| <a href="#">no</a> on page 1056                  | Removes or reverts this VLAN interface's settings to default                       |

| Commands                              | Description                                                                                                                                |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">shutdown</a> on page 1057 | Shuts down this VLAN interface                                                                                                             |
| <a href="#">use</a> on page 1058      | Associates an IP (IPv4 and IPv6) access list, bonjour-gw-discovery policy, and an IPv6-route-advertisement policy with this VLAN interface |

## crypto

[interface-config-vlan-instance](#) on page 1045

Associates an existing and configured VPN crypto map with this VLAN interface.

Crypto map entries are sets of configuration parameters for encrypting packets that pass through the VPN tunnel. For more information on crypto maps, see [crypto-map-config-commands](#) on page 955.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
crypto map <CRYPTO-MAP-NAME>
```

### Parameters

```
crypto map <CRYPTO-MAP-NAME>
```

|                                    |                                                                                                                                                                                                                    |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>map &lt;CRYPTO-MAP-NAME&gt;</b> | Attaches a crypto map to the selected VLAN interface. The crypto map should be existing and configured. <ul style="list-style-type: none"> <li>• &lt;CRYPTO-MAP-NAME&gt; - Specify the crypto map name.</li> </ul> |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Example

```
nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#crypto map map1

nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#show context
interface vlan8
crypto map map1
nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#
```

### Related Commands

|                                 |                                                              |
|---------------------------------|--------------------------------------------------------------|
| <a href="#">no</a> on page 1056 | Disables or reverts interface VLAN settings to their default |
|---------------------------------|--------------------------------------------------------------|

## description

[interface-config-vlan-instance](#) on page 1045

Defines this VLAN interface's description. Use this command to provide additional information about the VLAN.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

**description** <WORD>

#### Parameters

description <WORD>

|                                           |                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>description</b><br><b>&lt;WORD&gt;</b> | Configures a description for this VLAN interface (should not exceed 64 characters in length) <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specify a description unique to the VLAN's specific configuration, to help differentiate it from other VLANs with similar configurations.</li> </ul> |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Example

```
nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#description "This VLAN interface is configured for the Sales Team"
```

```
nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#show context
interface vlan8
description "This VLAN interface is configured for the Sales Team"
crypto map map1
nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#
```

#### Related Commands

|                        |                                        |
|------------------------|----------------------------------------|
| <b>no</b> on page 1056 | Removes the VLAN interface description |
|------------------------|----------------------------------------|

## dhcp

[interface-config-vlan-instance](#) on page 1045

Enables inclusion of optional fields (client identifier) in DHCP client requests. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

**dhcp client include client-identifier**

#### Parameters

dhcp client include client-identifier

|                                                                   |                                                                |
|-------------------------------------------------------------------|----------------------------------------------------------------|
| <b>dhcp client</b><br><b>include client-</b><br><b>identifier</b> | Enables inclusion of client identifier in DHCP client requests |
|-------------------------------------------------------------------|----------------------------------------------------------------|

### Example

```
nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#dhcp client include client-identifier
```

```
nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#show context
interface vlan8
 dhcp client include client-identifier
nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#
```

### Related Commands

|                                 |                                                                 |
|---------------------------------|-----------------------------------------------------------------|
| <a href="#">no</a> on page 1056 | Disables inclusion of client identifier in DHCP client requests |
|---------------------------------|-----------------------------------------------------------------|

## dhcp-relay-incoming

[interface-config-vlan-instance](#) on page 1045

Allows an onboard DHCP server to respond to relayed DHCP packets. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

**dhcp-relay-incoming**

### Parameters

None

### Example

```
nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#dhcp-relay-incoming
```

```
nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#show context
interface vlan8
 description "This VLAN interface is configured for the Sales Team"
 crypto map map1
 dhcp-relay-incoming
nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#
```

### Related Commands

|                                 |                                                              |
|---------------------------------|--------------------------------------------------------------|
| <a href="#">no</a> on page 1056 | Disables or reverts interface VLAN settings to their default |
|---------------------------------|--------------------------------------------------------------|

## ip

[interface-config-vlan-instance](#) on page 1045

Configures the VLAN interface's IP settings

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000

- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ip [address|dhcp|helper-address|nat|ospf]
```

```
ip helper-address <IP>
```

```
ip address [<IP/M>|<NETWORK-ALIAS-NAME>|dhcp|zeroconf]
```

```
ip address [<IP/M>|<NETWORK-ALIAS-NAME>|zeroconf] {secondary}
```

```
ip address dhcp
```

```
ip dhcp client request options all
```

```
ip nat [inside|outside]
```

```
ip ospf [authentication|authentication-key|bandwidth|cost|message-digest-key|priority]
```

```
ip ospf authentication [message-digest|null|simple-password]
```

```
ip ospf authentication-key simple-password [0 <WORD>|2 <WORD>]
```

```
ip ospf [bandwidth <1-10000000>|cost <1-65535>|priority <0-255>]
```

```
ip ospf message-digest-key key-id <1-255> md5 [0 <WORD>|2 <WORD>]
```

Parameters

```
ip helper-address <IP>
```

|                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>helper-address</b><br><b>&lt;IP&gt;</b> | <p>Enables DHCP and BOOTP requests forwarding for a set of clients. Configure a helper address on the VLAN interface connected to the client. The helper address should specify the address of the BOOTP or DHCP servers to receive the requests. If you have multiple servers, configure one helper address for each server.</p> <ul style="list-style-type: none"> <li>• &lt;IP&gt; - Specify the IP address of the DHCP or BOOTP server.</li> </ul> |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
ip address [<IP/M>|<NETWORK-ALIAS-NAME>|zeroconf] {secondary}
```

|                                   |                                                                                                                                                                                                                                                                    |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>address</b>                    | Sets the VLAN interface's IP address                                                                                                                                                                                                                               |
| <b>&lt;IP/M&gt;</b>               | <p>Specifies the interface IP address in the A.B.C.D/M format</p> <ul style="list-style-type: none"> <li>• secondary - Optional. Sets the specified IP address as a secondary address</li> </ul>                                                                   |
| <b>&lt;NETWORK-ALIAS-NAME&gt;</b> | <p>Uses a pre-defined network alias to provide this VLAN interface's IP address. Specify the network alias name.</p> <ul style="list-style-type: none"> <li>• secondary - Optional. Sets the network-alias provided IP address as the secondary address</li> </ul> |

|                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>zeroconf</b><br><b>{secondary}</b> | Uses Zero Configuration Networking (zeroconf) to generate an IP address for this interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|                                       | <p>Zero configuration can be a means of providing a primary or secondary IP addresses for the virtual interface. Zero configuration (or zero config) is a wireless connection utility included with Microsoft Windows XP and later as a service dynamically selecting a network to connect based on a user's preferences and various default settings. Zero config can be used instead of a wireless network utility from the manufacturer of a computer's wireless networking device.</p> <ul style="list-style-type: none"> <li>• secondary - Optional. Sets the generated IP address as a secondary address</li> </ul> |

ip address dhcp

|                |                                                                    |
|----------------|--------------------------------------------------------------------|
| <b>address</b> | Sets the VLAN interface's IP address                               |
| <b>dhcp</b>    | Uses a DHCP client to obtain an IP address for this VLAN interface |

ip dhcp client request options all

|                |                                                                  |
|----------------|------------------------------------------------------------------|
| <b>dhcp</b>    | Uses a DHCP client to configure a request on this VLAN interface |
| <b>client</b>  | Configures a DHCP client                                         |
| <b>request</b> | Configures DHCP client request                                   |
| <b>options</b> | Configures DHCP client request options                           |
| <b>all</b>     | Configures all DHCP client request options                       |

ip nat [inside|outside]

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>nat [inside outside]</b> | <p>Defines NAT settings for the VLAN interface. NAT is disabled by default.</p> <ul style="list-style-type: none"> <li>• inside - Enables NAT on the inside interface. The inside network is transmitting data over the network to the intended destination. On the way out, the source IP address is changed in the header and replaced by the (public) IP address.</li> <li>• outside - Enables NAT on the outside interface. Packets passing through the NAT on the way back to the managed LAN are searched against the records kept by the NAT engine. There, the destination IP address is changed back to the specific internal private class IP address in order to reach the LAN over the network.</li> </ul> |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

ip ospf authentication [message-digest|null|simple-password]

|                            |                                                                                               |
|----------------------------|-----------------------------------------------------------------------------------------------|
| <b>ospf authentication</b> | Configures OSPF authentication scheme. Options are message-digest, null, and simple-password. |
| <b>message-digest</b>      | Configures md5 based authentication                                                           |
| <b>null</b>                | No authentication required                                                                    |
| <b>simple-password</b>     | Configures simple password based authentication                                               |

ip ospf authentication-key simple-password [0 <WORD>|2 <WORD>]

|                                               |                                                                                                                                                                                                          |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ospf authentication-key</b>                | Configures an OSPF authentication key                                                                                                                                                                    |
| <b>simple-password</b><br>[0 <WORD> 2 <WORD>] | Configures a simple password OSPF authentication key <ul style="list-style-type: none"> <li>• 0 &lt;WORD&gt; - Configures clear text key</li> <li>• 2 &lt;WORD&gt; - Configures encrypted key</li> </ul> |

```
ip ospf [bandwidth <1-10000000>|cost <1-65535>|priority <0-255>]
```

|                                  |                                                                                                                                                                                               |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>bandwidth</b><br><1-10000000> | Configures bandwidth for the physical port mapped to this layer 3 interface <ul style="list-style-type: none"> <li>• &lt;1-10000000&gt; - Specify the bandwidth from 1 - 10000000.</li> </ul> |
| <b>cost</b> <1-65535>            | Configures OSPF cost <ul style="list-style-type: none"> <li>• &lt;1-65535&gt; - Specify OSPF cost value from 1 - 65535.</li> </ul>                                                            |
| <b>priority</b><br><0-255>       | Configures OSPF priority <ul style="list-style-type: none"> <li>• &lt;0-255&gt; - Specify OSPF priority value from 0 - 255.</li> </ul>                                                        |

```
ip ospf message-digest-key key-id <1-255> md5 [0 <WORD>|2 <WORD>]
```

|                                |                                                                                                                                                                        |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ospf message-digest</b>     | Configures message digest authentication parameters                                                                                                                    |
| <b>key-id</b> <1-255>          | Configures message digest authentication key ID from 0 - 255                                                                                                           |
| <b>md5</b> [0 <WORD> 2 <WORD>] | Configures md5 key <ul style="list-style-type: none"> <li>• 0 &lt;WORD&gt; - Configures clear text key</li> <li>• 2 &lt;WORD&gt; - Configures encrypted key</li> </ul> |

#### Example

```
nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#ip address 10.0.0.1/8

nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#ip nat inside

nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#ip helper-address 172.16.10.3

nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#ip dhcp client request options all

nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#show context
interface vlan8
description "This VLAN interface is configured for the Sales Team"
ip address 10.0.0.1/8
ip dhcp client request options all
ip helper-address 172.16.10.3
ip nat inside
crypto map map1
dhcp-relay-incoming
nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#
```

#### Related Commands

|                        |                                                 |
|------------------------|-------------------------------------------------|
| <b>no</b> on page 1056 | Removes or resets IP settings on this interface |
|------------------------|-------------------------------------------------|

ipv6

[interface-config-vlan-instance](#) on page 1045

Configures the VLAN interface's IPv6 settings

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ipv6 [accept | address | dhcp | enable | enforce-dad | mtu | redirects | request-dhcpv6-options | router-advertisements]
```

```
ipv6 accept ra {(no-default-router|no-hop-limit|no-mtu)}
```

```
ipv6 address [<IPv6/M> | autoconfig | eui-64 | link-local | prefix-from-provider]
```

```
ipv6 address [<IPv6/M> | autoconfig]
```

```
ipv6 address eui-64 [<IPv6/M> | prefix-from-provider <WORD> <IPv6-PREFIX/PREFIX-LENGTH>]
```

```
ipv6 address prefix-from-provider <WORD> <HOST-PORITION/LENGTH>
```

```
ipv6 address link-local <LINK-LOCAL-ADD>
```

```
ipv6 dhcp [client [information | prefix-from-provider <WORD>] | relay destination <DEST-IPv6-ADD>]
```

```
ipv6 [enable | enforce-dad | mtu <1280-1500> | redirects | request-dhcpv6-options]
```

```
ipv6 router-advertisements [prefix <IPv6-PREFIX> | prefix-from-provider <WORD>] {no-autoconfig | off-link | site-prefix | valid-lifetime}
```

Parameters

```
ipv6 accept ra {(no-default-router|no-hop-limit|no-mtu)}
```

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipv6 accept ra</b>    | Enables processing of router advertisements (RAs) on this VLAN interface. This option is enabled by default.<br>When enabled, IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery protocol via ICMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to the request with a router advertisement packet containing Internet layer configuration parameters. |
| <b>no-default-router</b> | Optional. Disables inclusion of routers on this interface in the default router selection process. This option is disabled by default.                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>no-hop-limit</b>      | Optional. Disables the use of RA advertised hop-count value on this interface. This option is disabled by default.                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>no-mtu</b>            | Optional. Disables the use of RA advertised MTU value on this interface. This option is disabled by default.                                                                                                                                                                                                                                                                                                                                                                                                                                             |

```
ipv6 address [<IPv6/M> | autoconfig]
```



|                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipv6 address</b><br>[<IPv6/M>  <br><b>autoconfig</b> ] | <p>Configures IPv6 address related settings on this VLAN interface</p> <ul style="list-style-type: none"> <li>• &lt;IPv6&gt; – Specify the non-link local static IPv6 address and prefix length of the interface in the X::X:X/M format.</li> <li>• autoconfig – Enables stateless auto-configuration of IPv6 address, based on the prefixes received from RAs (with auto-config flag set). These prefixes are used to auto-configure the IPv6 address. This option is enabled by default. Use the no &gt; ipv6 &gt; address &gt; autoconfig command to negate the use of prefixes received in RAs.</li> </ul> |
|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
ipv6 address eui-64 [<IPv6/M>|prefix-from-provider <WORD> <IPv6-PREFIX/PREFIX-LENGTH>]
```

|                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• <b>ipv6 address eui-64</b></li> </ul> | <p>Configures the IPv6 prefix and prefix length. This prefix is used to auto-generate the static IPv6 address (for this interface) in the modified Extended Unique Identifier (EUI)-64 format.</p> <p>Implementing the IEEE's 64-bit EUI64 format enables a host to automatically assign itself a unique 64-bit IPv6 interface identifier, without manual configuration or DHCP. This is accomplished on a virtual interface by referencing the already unique 48-bit MAC address, and reformatting it to match the EUI-64 specification.</p> <p>In the EUI-64 IPv6 address the prefix and host portions are each 64 bits in length.</p> |
|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;IPv6/M&gt;</b> | <p>Specify the IPv6 prefix and prefix length. This configured value is used as the prefix portion of the auto-generated IPv6 address, and the host portion is derived from the MAC address of the interface.</p> <p>Any bits of the configured value exceeding the prefix-length "M" are ignored and replaced by the host portion derived from the MAC address.</p> <p>For example:<br/>Prefix portion provided using this command: <code>ipv6 &gt; address &gt; eui-64 &gt; 2004:b055:15:dead::1111/64</code>.</p> <p>Host portion derived using the interface's MAC address (00-15-70-37-FB-5E):<br/>215:70ff:fe37:fb5e</p> <p>Auto-configured IPv6 address using the above prefix and host portions:<br/>2004:b055:15:dead:215:70ff:fe37:fb5e/64</p> <p>In this example, the host part "::1111" is ignored and replaced with the modified eui-64 formatted host address.</p> |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>prefix-from-provider &lt;WORD&gt;</b><br><b>&lt;IPv6-PREFIX/PREFIX-LENGTH&gt;</b> | <p>Configures the "prefix-from-provider" named object and the associated IPv6 prefix and prefix length. This configured value is used as the prefix portion of the auto-generated IPv6 address, and the host portion is derived from the MAC address of the interface.</p> <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the IPv6 "prefix-from-provider" object's name. This is the IPv6 general prefix (32 character maximum) name provided by the Internet service provider.</li> </ul> |
|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• &lt;IPv6-PREFIX/PREFIX-LENGTH&gt; – Specify the IPv6 address subnet and host parts along with prefix length (site-renumbering).</li> </ul> <p>For example:<br/>Prefix portion provided using this command: <code>ipv6 &gt; address &gt; eui-64 &gt; prefix-from-provider &gt; ISP1-prefix &gt; 2002::/64</code></p> <p>Host portion derived using the interface's MAC address (00-15-70-37-FB-5E):<br/>215:70ff:fe37:fb5e</p> <p>Auto-configured IPv6 address using the above prefix and host portions:<br/>2002::215:70ff:fe37:fb5e/64</p> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
ipv6 address prefix-from-provider <WORD> <HOST-PORZION/LENGTH>]
```



|                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipv6 address</b>                                                  | Configures the IPv6 address related settings on this VLAN interface                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>prefix-from-provider &lt;WORD&gt; &lt;HOST-PORTION/LENGTH&gt;</b> | <p>Configures the “prefix-from-provider” named object and the host portion of the IPv6 interface address. The prefix derived from the specified “prefix-from-provider” and the host portion (second parameter) are combined together (using the prefix-length of the specified “prefix-from-provider”) to generate the interface’s IPv6 address.</p> <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Provide the “prefix-from-provider” object’s name. This is the IPv6 general prefix (32 character maximum) name provided by the service provider.</li> <li>• &lt;HOST-PORTION/LENGTH&gt; - Provide the subnet number, host portion, and prefix length used to form the actual address along with the prefix derived from the “prefix-from-provider” object identified by the &lt;WORD&gt; keyword.</li> </ul> |

ipv6 address link-local <LINK-LOCAL-ADD>

|                                          |                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipv6 address</b>                      | Configures the IPv6 address related settings on this VLAN interface                                                                                                                                                                                                                                                                                                            |
| <b>link-local &lt;LINK-LOCAL-ADD&gt;</b> | <p>Configures IPv6 link-local address on this interface. The configured value overrides the default link-local address derived from the interface’s MAC address. Use the <b>no &gt; ipv6 &gt; link-local</b> command to restore the default link-local address derived from MAC address.</p> <p>It is mandatory for an IPv6 interface to always have a link-local address.</p> |

ipv6 dhcp [client [information|prefix-from-provider <WORD>]|relay destination <DEST-IPv6-ADD>]

|                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipv6 dhcp client [information prefix-from-provider &lt;WORD&gt;]</b> | <p>Configures DHCPv6 client-related settings on this VLAN interface</p> <ul style="list-style-type: none"> <li>• information - Configures stateless DHCPv6 client on this interface. When enabled, the device can request configuration information from the DHCPv6 server using stateless DHCPv6. This option is disabled by default.</li> <li>• prefix-from-provider - Configures prefix-delegation client on this interface. Enter the IPv6 general prefix (32 character maximum) name provided by the service provider. This option is disabled by default.</li> </ul>                                                                                                                                                                                                                                                                                                                                                     |
| <b>relay destination &lt;DEST-IPv6-ADD&gt;</b>                          | <p>Enables DHCPv6 packet forwarding on this VLAN interface</p> <ul style="list-style-type: none"> <li>• destination - Forwards DHCPv6 packets to a specified DHCPv6 relay <ul style="list-style-type: none"> <li>• &lt;DEST-IPv6-ADD&gt; - Specify the destination DHCPv6 relay’s address.</li> </ul> </li> </ul> <p>DHCPv6 relay enhances an extended DHCP relay agent by providing support in IPv6. DHCP relays exchange messages between a DHCPv6 server and client. A client and relay agent exist on the same link. When a DHCP request is received from the client, the relay agent creates a relay forward message and sends it to a specified server address. If no addresses are specified, the relay agent forwards the message to all DHCP server relay multicast addresses. The server creates a relay reply and sends it back to the relay agent. The relay agent then sends back the response to the client.</p> |

ipv6 [enable|enforce-dad|mtu <1280-1500>|redirects|request-dhcp-options]

|                              |                                                                                                                                                                                                                         |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipv6</b>                  | Configures IPv6 settings on this VLAN interface                                                                                                                                                                         |
| <b>enable</b>                | Enables IPv6 on this interface. This option is disabled by default.                                                                                                                                                     |
| <b>enforce-dad</b>           | Enforces Duplicate Address Detection (DAD) on wired ports. This option is enabled by default.                                                                                                                           |
| <b>mtu &lt;1280-1500&gt;</b> | <p>Configures the Maximum Transmission Unit (MTU) for IPv6 packets on this interface</p> <ul style="list-style-type: none"> <li>• &lt;1280-1500&gt; - Specify a value from 1280 - 1500. The default is 1500.</li> </ul> |

|                             |                                                                                                |
|-----------------------------|------------------------------------------------------------------------------------------------|
| <b>redirects</b>            | Enables ICMPv6 redirect messages sending on this interface. This option is enabled by default. |
| <b>request-dhcp-options</b> | Requests options from DHCPv6 server on this interface. This option is disabled by default.     |

```
ipv6 router-advertisements [prefix <IPv6-PREFIX>|prefix-from-provider <WORD>] {no-
autoconfig|off-link|site-prefix <SITE-PREFIX>|valid-lifetime}
```

|                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipv6 router-advertisements</b>                                              | Configures IPv6 RA related settings on this VLAN interface                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>prefix &lt;IPv6-PREFIX&gt;</b>                                              | Configures a static prefix and its related parameters. The configured value is advertised on RAs. <ul style="list-style-type: none"> <li>• &lt;IPv6-PREFIX&gt; - Specify the IPv6 prefix.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>prefix-from-provider &lt;WORD&gt;</b>                                       | Configures a static "prefix-from-provider" named object and its related parameters on this VLAN interface. The configured value is advertised on RAs. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specify the "prefix-from-provider" named object's name</li> </ul>                                                                                                                                                                                                                                                                                                         |
| <b>no-autoconfig</b>                                                           | This parameter is common to the "general-prefix", "prefix", and "prefix-from-provider" keywords. <ul style="list-style-type: none"> <li>• no-autoconfig - Optional. Disables the setting of the auto configuration flag in the prefix. When configured, the configured prefixes are not used for IPv6 address generation. The autoconfiguration option is enabled by default. Using no-autoconfig disables it.</li> </ul>                                                                                                                                                               |
| <b>off-link</b>                                                                | This parameter is common to the "general-prefix", "prefix", and "prefix-from-provider" keywords. <ul style="list-style-type: none"> <li>• off-link - Optional. Disables the setting of the on-link flag in the prefix. The on-link option is enabled by default. Using off-link disables it.</li> </ul>                                                                                                                                                                                                                                                                                 |
| <b>site-prefix &lt;SITE-PREFIX&gt;</b>                                         | This parameter is common to the "general-prefix", "prefix", and "prefix-from-provider" keywords. <ul style="list-style-type: none"> <li>• site-prefix &lt;SITE-PREFIX&gt; - Configures subnet (site) prefix</li> </ul>                                                                                                                                                                                                                                                                                                                                                                  |
| <b>valid-lifetime [&lt;30-4294967294&gt; at infinite] (preferred-lifetime)</b> | This parameter is common to the "general-prefix", "prefix", and "prefix-from-provider" keywords. <ul style="list-style-type: none"> <li>• valid-lifetime - Configures the valid lifetime for the prefix</li> <li>• preferred-lifetime - Configures preferred lifetime for the prefix</li> <li>• &lt;30-4294967294&gt; - Configures the valid/preferred lifetime in seconds <ul style="list-style-type: none"> <li>• at - Configures expiry time and date of the valid/preferred lifetime</li> <li>infinite - Configures the valid/preferred lifetime as infinite</li> </ul> </li> </ul> |

#### Example

```
nx9500-6C8809(config-profile-test-if-vlan4)#ipv6 enable

nx9500-6C8809(config-profile-test-if-vlan4)#ipv6 accept ra no-mtu

rfs6000-81742D(config-profile-test-if-vlan4)#ipv6 address eui-64 prefix-from-provider ISP1-
prefix 2002::/64

nx9500-6C8809(config-profile-test-if-vlan4)#show context
interface vlan4
 ipv6 enable
 ipv6 address eui-64 prefix-from-provider ISP1-prefix 2002::/64
```

```
ipv6 accept ra no-mtu
nx9500-6C8809(config-profile-test-if-vlan4)#
```

#### Related Commands

|                                 |                                                        |
|---------------------------------|--------------------------------------------------------|
| <a href="#">no</a> on page 1056 | Removes or resets IPv6 settings on this VLAN interface |
|---------------------------------|--------------------------------------------------------|

no

[interface-config-vlan-instance](#) on page 1045

Negates a command or reverts to defaults. The no command, when used in the Config Interface VLAN mode, negates VLAN interface settings or reverts them to their default.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
no [crypto|description|dhcp|dhcp-relay-incoming|ip|ipv6|shutdown|use]
```

```
no dhcp client include client-identifier
```

```
no [crypto map|description|dhcp-relay-incoming|shutdown]
```

```
no ip [address|dhcp|helper-address|nat|ospf]
```

```
no ip [helper-address <IP>|nat]
```

```
no ip address {<IP/M> {secondary}|<NETWORK-ALIAS-NAME> {secondary}}/dhcp/
zeroconf {secondary}}
```

```
no ip dhcp client request options all
```

```
no ip ospf [authentication|authentication-key|bandwidth|cost|message-
digest-key| priority]
```

```
no ipv6 [accept|address|dhcp|enable|enforce-dad|mtu|redirects|request-
dhcpv6-options|router-advertisement]
```

```
no ipv6 [accept ra|enable|enforce-dad|mtu|redirects|request-dhcpv6-
options]
```

```
no ipv6 address [<IPv6/M>|autoconfig|eui-64|link-local|prefix-from-
provider]
```

```
no ipv6 dhcp [client|relay]
```

```
no ipv6 router-advertisement [prefix <WORD>|prefix-from-provider <WORD>]
```

```
no use [bonjour-gw-discovery-policy>|ip-access-list in|ipv6-access-list
in|ipv6-router-advertisement-policy|url-filter]
```

#### Parameters

```
no <PARAMETERS>
```

|                                        |                                                                                  |
|----------------------------------------|----------------------------------------------------------------------------------|
| <b>no</b><br><b>&lt;PARAMETERS&gt;</b> | Removes or reverts this VLAN interface's settings based on the parameters passed |
|----------------------------------------|----------------------------------------------------------------------------------|

## Example

The following example shows the VLAN interface settings before the 'no' commands are executed:

```
nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#show context
interface vlan8
description "This VLAN interface is configured for the Sales Team"
ip address 10.0.0.1/8
ip dhcp client request options all
ip helper-address 172.16.10.3
ip nat inside
crypto map map1
dhcp-relay-incoming
nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#

nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#no crypto map
nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#no description
nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#no dhcp-relay-incoming
nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#no ip dhcp client request options
all
```

The following example shows the VLAN interface settings after the 'no' commands are executed:

```
nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#show context
interface vlan8
ip address 10.0.0.1/8
ip helper-address 172.16.10.3
ip nat inside
nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#
```

## shutdown

[interface-config-vlan-instance](#) on page 1045

Shuts down the selected interface. Use the no shutdown command to enable an interface.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

## Syntax

**shutdown**

## Parameters

None

## Example

```
nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#shutdown

nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#show context
interface vlan8
ip address 10.0.0.1/8
ip helper-address 172.16.10.3
```

```
shutdown
nx9500-6c8809(config-profile-default-rfs4000-if-vlan8)#
```

#### Related Commands

|                                 |                                                              |
|---------------------------------|--------------------------------------------------------------|
| <a href="#">no</a> on page 1056 | Disables or reverts interface VLAN settings to their default |
|---------------------------------|--------------------------------------------------------------|

use

[interface-config-vlan-instance](#) on page 1045

Associates an IP (IPv4 and IPv6) access list, bonjour-gw-discovery policy, and an IPv6-router-advertisement policy with this VLAN interface

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
use [bonjour-gw-discovery-policy <POLICY-NAME>|ip-access-list in <IP-ACL-NAME>|ipv6-access-list in <IPv6-ACL-NAME>|ipv6-router-advertisement-policy <POLICY-NAME>|url-filter <URL-FILTER-NAME>]
```

#### Parameters

```
use [bonjour-gw-discovery-policy <POLICY-NAME>|ip-access-list in <IP-ACL-NAME>|ipv6-access-list in <IPv6-ACL-NAME>|ipv6-router-advertisement-policy <POLICY-NAME>|url-filter <URL-FILTER-NAME>]
```

|                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>bonjour-gw-discovery-policy &lt;POLICY-NAME&gt;</b>   | Uses an existing Bonjour GW Discovery policy with this VLAN interface. When associated, the Bonjour GW Discovery policy is applied for the Bonjour requests coming over the VLAN interface. <ul style="list-style-type: none"><li>• &lt;POLICY-NAME&gt; - Specify the Bonjour GW Discovery policy name (should be existing and configured).</li></ul> For more information on Bonjour GW Discovery policy, see <a href="#">bonjour-gw-discovery-policy</a> on page 287. |
| <b>ip-access-list in &lt;IP-ACCESS-LIST-NAME&gt;</b>     | Uses a specified IPv4 access list with this interface <ul style="list-style-type: none"><li>• in - Applies IPv4 ACL to incoming packets</li><li>• &lt;IP-ACCESS-LIST-NAME&gt; - Specify the IPv4 access list name.</li></ul>                                                                                                                                                                                                                                            |
| <b>ipv6-access-list in &lt;IPv6-ACCESS-LIST-NAME&gt;</b> | Uses a specified IPv6 access list with this interface <ul style="list-style-type: none"><li>• in - Applies IPv6 ACL to incoming packets</li><li>• &lt;IPv6-ACCESS-LIST-NAME&gt; - Specify the IPv6 access list name.</li></ul>                                                                                                                                                                                                                                          |

|                                                             |                                                                                                                                                                                                                                              |
|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipv6-router-advertisement-policy &lt;POLICY-NAME&gt;</b> | Uses an existing IPv6 router advertisement policy with this VLAN interface. <ul style="list-style-type: none"> <li>• &lt;POLICY-NAME&gt; - Specify the IPv6 router advertisement policy name (should be existing and configured).</li> </ul> |
| <b>url-filter &lt;URL-FILTER-NAME&gt;</b>                   | Enforces URL filtering on this VLAN interface by associating a URL filter <ul style="list-style-type: none"> <li>• &lt;URL-FILTER-NAME&gt; - Specify the URL filter name (should be existing and configured).</li> </ul>                     |

#### Example

```
nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#use ip-access-list in test
```

```
nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#show context
```

```
interface vlan8
 ip address 10.0.0.1/8
 use ip-access-list in test
 ip helper-address 172.16.10.3
```

```
nx9500-6C8809(config-profile-default-rfs4000-if-vlan8)#
```

#### Related Commands

|                        |                                                              |
|------------------------|--------------------------------------------------------------|
| <b>no</b> on page 1056 | Disables or reverts interface VLAN settings to their default |
|------------------------|--------------------------------------------------------------|

## interface-config-port-channel-instance

[interface](#) on page 1013

Profiles can utilize customized port channel configurations as part of their interface settings. Existing port channel profile configurations can be overridden as they become obsolete for specific device deployments.

The following example uses the config-profile-testNX9000 instance to configure a port-channel interface:

```
nx9500-6C8809(config-profile-testNX9000)#interface port-channel 1
nx9500-6C8809(config-profile-testNX9000-if-port-channell)# Port Channel Mode commands:
```

```
description Port description
duplex Set duplex to interface
ip Internet Protocol (IP)
ipv6 Internet Protocol version 6 (IPv6)
no Negate a command or set its defaults
port-channel Portchannel commands
qos Quality of service
remove-override Remove configuration item override from the device (so
 profile value takes effect)
shutdown Shutdown the selected interface
spanning-tree Spanning tree commands
speed Configure speed
switchport Set switching mode characteristics
use Set setting to use
```

```
clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
```

show Show running system information  
 write Write running configuration to memory or terminal

nx9500-6C8809(config-profile-testNX9000-if-port-channell)#

| Commands                                   | Description                                                                                     |
|--------------------------------------------|-------------------------------------------------------------------------------------------------|
| <a href="#">description</a> on page 1060   | Configures a brief description for this port-channel interface                                  |
| <a href="#">duplex</a> on page 1061        | Configures the duplex-mode (that is the data transmission mode) for this port-channel interface |
| <a href="#">ip</a> on page 1061            | Configures ARP and DHCP related security parameters on this port-channel interface              |
| <a href="#">ipv6</a> on page 1062          | Configures IPv6 related parameters on this port-channel interface                               |
| <a href="#">no</a> on page 1065            | Removes or reverts to default this port-channel interface's settings                            |
| <a href="#">shutdown</a> on page 1066      | Shutsdown this port-channel interface                                                           |
| <a href="#">spanning-tree</a> on page 1066 | Configures spanning-tree related parameters on this port channel interface                      |
| <a href="#">speed</a> on page 1068         | Configures the speed at which this port-channel interface receives and transmits data           |
| <a href="#">switchport</a> on page 1069    | Configures the packet switching parameters for this port-channel interface                      |
| <a href="#">use</a> on page 1071           | Configures access controls on this port-channel interface                                       |

description

[interface-config-port-channel-instance](#) on page 1059

Configures a brief description for this port channel interface

Supported in the following platforms:

- Wireless Controllers – RFS4000
- Service Platforms – NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

**description** <LINE>

Parameters

**description** <LINE>

|                                           |                                                                                                                                                                                                                                                         |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>description</b><br><b>&lt;LINE&gt;</b> | Configures a description for this port-channel interface that uniquely identifies it from other port channel interfaces <ul style="list-style-type: none"> <li>• &lt;LINE&gt; - Provide a description not exceeding 64 characters in length.</li> </ul> |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Example

```
nx9500-6C8809(config-profile-testNX9000-if-port-channell)#description "This port
-channel is for enabling dynamic LACP."
```

```
nx9500-6C8809(config-profile-testNX9000-if-port-channell)#show context
interface port-channell
nx9500-6C8809(config-profile-testNX9000-if-port-channell)#
```



## Related Commands

|                                 |                                                   |
|---------------------------------|---------------------------------------------------|
| <a href="#">no</a> on page 1065 | Removes this port-channel interface's description |
|---------------------------------|---------------------------------------------------|

## duplex

[interface-config-port-channel-instance](#) on page 1059

Configures the duplex-mode (that is the data transmission mode) for this port channel interface

Supported in the following platforms:

- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
duplex [auto|half|full]
```

### Parameters

```
duplex [auto|half|full]
```

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>duplex [auto half full]</b> | Configures the mode of data transmission as auto, full, or half                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|                                | <ul style="list-style-type: none"><li>• auto – Select this option to enable the controller, service platform, or access point to dynamically duplex as port channel performance needs dictate. This is the default setting.</li><li>• full – Select this option to simultaneously transmit data to and from the port channel.</li><li>• half – Select this option to send data over the port channel, then immediately receive data from the same direction in which the data was transmitted.</li></ul> |

### Example

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#duplex full

nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#show context
interface port-channel1
 description "This port-channel is for enabling dynamic LACP."
 duplex full
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#
```

## Related Commands

|                                 |                                                     |
|---------------------------------|-----------------------------------------------------|
| <a href="#">no</a> on page 1065 | Reverts the duplex-mode to the default value (auto) |
|---------------------------------|-----------------------------------------------------|

## ip

[interface-config-port-channel-instance](#) on page 1059

Configures ARP and DHCP related security parameters on this port-channel interface

Supported in the following platforms:

- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
ip [arp|dhcp]
```

```
ip arp [header-mismatch-validation|trust]
```

```
ip dhcp trust
```

Parameters

```
ip arp [header-mismatch-validation|trust]
```

|                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ip arp</b><br><b>[header-</b><br><b>mismatch-</b><br><b>validation</b><br><b> </b><br><b>trust]</b> | Configures ARP related parameters on this port-channel interface <ul style="list-style-type: none"><li>• header-mismatch-validation – Enables a source MAC mismatch check in both the ARP and ethernet headers. This option is enabled by default.</li><li>• trust – Enables ARP trust on this port channel. If enabled, ARP packets received on this port are considered trusted, and information from these packets is used to identify rogue devices. This option is disabled by default.</li></ul> |
|--------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
ip dhcp trust
```

|                      |                                                                                                                                                                                                        |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ip dhcp trust</b> | Enables DHCP trust. If enabled, only DHCP responses are trusted and forwarded on this port channel, and a DHCP server can be connected only to a DHCP trusted port. This option is enabled by default. |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Example

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#ip arp trust
```

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#show context
```

```
interface port-channel1
 description "This port-channel is for enabling dynamic LACP."
 duplex full
 ip arp trust
```

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#
```

Related Commands

|                        |                                                                               |
|------------------------|-------------------------------------------------------------------------------|
| <b>no</b> on page 1065 | Removes or reverts to default the ARP and DHCP security parameters configured |
|------------------------|-------------------------------------------------------------------------------|

ipv6

[interface-config-port-channel-instance](#) on page 1059

Configures IPv6 related parameters on this port-channel interface

Supported in the following platforms:

- Wireless Controllers – RFS4000
- Service Platforms – NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ipv6 [dhcpv6|nd]
```

```
ipv6 dhcpv6 trust
```

```
ipv6 nd [header-mismatch-validation|raguard|trust]
```

Parameters

```
ipv6 dhcpv6 trust
```

|                          |                                                                                                                                                                                                         |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipv6 dhcpv6 trust</b> | Enables DHCPv6 trust. If enabled, only DHCPv6 responses are trusted and forwarded on this port channel, and a DHCPv6 server can be connected only to a trusted port. This option is enabled by default. |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
ipv6 nd [header-mismatch-validation|raguard|trust]
```

|                                                           |                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipv6 nd [header-mismatch-validation raguard trust]</b> | Configures IPv6 neighbor discovery (ND) parameters <ul style="list-style-type: none"> <li>header-mismatch-validation – Enables a mismatch check for the source MAC in both the ND header and link layer options. This option is disabled by default.</li> </ul> |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                |                                                                                                                                                                                                                                                                                           |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>raguard</b> | Enables router advertisements or IPv6 redirects from this port. Router advertisements are periodically sent to hosts or are sent in response to solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information. This option is enabled by default. |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|              |                                                                                                                                                                                                         |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>trust</b> | Enables DHCPv6 trust. If enabled, only DHCPv6 responses are trusted and forwarded on this port channel, and a DHCPv6 server can be connected only to a trusted port. This option is enabled by default. |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Example

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#ipv6 nd header-mismatch-validation
```

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#ipv6 nd trust
```

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#show context
interface port-channel1
description "This port-channel is for enabling dynamic LACP."
duplex full
ipv6 nd trust
ipv6 nd header-mismatch-validation
ip arp trust
```

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#
```

#### Related Commands

|                        |                                                                                          |
|------------------------|------------------------------------------------------------------------------------------|
| <b>no</b> on page 1065 | Removes or reverts to default the IPv6 related parameters on this port-channel interface |
|------------------------|------------------------------------------------------------------------------------------|

#### port-channel

[interface-config-port-channel-instance](#) on page 1059

Configures client load balancing parameters on this port-channel interface

Supported in the following platforms:

- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
port-channel load-balance [src-dst-ip|src-dst-mac]
```

#### Parameters

```
port-channel load-balance [src-dst-ip|src-dst-mac]
```

|                                                             |                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>port-channel load-balance [src-dst-ip   src-dst-mac]</b> | <p>Specifies whether port channel load balancing is conducted using a source/destination IP or a source/destination MAC.</p> <ul style="list-style-type: none"> <li>• src-dst-ip - Uses a source/destination IP to conduct client load balancing. This is the default setting.</li> <li>• src-dst-mac - Uses a source/destination MAC to conduct client load balancing</li> </ul> |
|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Example

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#port-channel load-balance src-dst-mac
```

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#show context
interface port-channel1
description "This port-channel is for enabling dynamic LACP."
duplex full
ipv6 nd trust
ipv6 nd header-mismatch-validation
ip arp trust
port-channel load-balance src-dst-mac
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#
```

#### Related Commands

|                        |                                                                                                   |
|------------------------|---------------------------------------------------------------------------------------------------|
| <b>no</b> on page 1065 | Removes or reverts to default the client load balancing parameters on this port-channel interface |
|------------------------|---------------------------------------------------------------------------------------------------|

## qos

[interface-config-port-channel-instance](#) on page 1059

Configures Quality of Service (QoS) related parameters on this port-channel interface

Supported in the following platforms:

- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
qos trust [802.1p | dscp]
```

#### Parameters

```
qos trust [802.1p | dscp]
```

|                                  |                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>qos trust [802.1p   dscp]</b> | <p>Configures the following QoS related parameters:</p> <ul style="list-style-type: none"> <li>• 802.1p - Trusts 802.1p class of service (COS) values ingressing on this port channel. This option is enabled by default.</li> <li>• dscp - Trusts IP DSCP QOS values ingressing on this port channel. This option is enabled by default.</li> </ul> |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Example

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#qos trust dscp
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#show context
```

#### Related Commands

|                        |                                                                              |
|------------------------|------------------------------------------------------------------------------|
| <b>no</b> on page 1065 | Removes the QoS related parameters configured on this port-channel interface |
|------------------------|------------------------------------------------------------------------------|

no

[interface-config-port-channel-instance](#) on page 1059

Removes or reverts to default this port-channel interface's settings

Supported in the following platforms:

- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no beacon [description|duplex|ip|ipv6|port-channel|qos|shutdown|spanning-tree| speed|switchport|use]
```

Parameters

```
no <PARAMETERS>
```

|                                        |                                                                                                                                                                                                     |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>no</b><br><b>&lt;PARAMETERS&gt;</b> | Removes or reverts to default this port-channels interface's settings based on the parameters passed <ul style="list-style-type: none"><li>• &lt;PARAMETERS&gt; - Specify the parameters.</li></ul> |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Example

The following example shows the port-channel interface's interface settings before the 'no' commands are executed:

```
nx9500-6C8809(config-profile-testNX9000-if-port-channell)#show context
description "This port-channel is for enabling dynamic LACP."
 speed 100
 duplex full
 switchport mode trunk
 switchport trunk native vlan 1
 no switchport trunk native tagged
 switchport trunk allowed vlan 1
 use ip-access-list in BROADCAST-MULTICAST-CONTROL
 ipv6 nd trust
 ipv6 nd header-mismatch-validation
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree bpdufilter enable
 spanning-tree mst 1 port-priority 1
 spanning-tree mst 1 cost 20000
 ip arp trust
 port-channel load-balance src-dst-mac
nx9500-6C8809(config-profile-testNX9000-if-port-channell)#
```

```
nx9500-6C8809(config-profile-testNX9000-if-port-channell)#no duplex
nx9500-6C8809(config-profile-testNX9000-if-port-channell)#no ip arp trust
nx9500-6C8809(config-profile-testNX9000-if-port-channell)#no ipv6 nd trust
nx9500-6C8809(config-profile-testNX9000-if-port-channell)#no port-channel load-balance
```

The following example shows the port-channel interface's interface settings after the 'no' commands are executed:

```
nx9500-6C8809(config-profile-testNX9000-if-port-channell)#show context
interface port-channell
 description "This port-channel is for enabling dynamic LACP."
 speed 100
 switchport mode trunk
```

```

switchport trunk native vlan 1
no switchport trunk native tagged
switchport trunk allowed vlan 1
use ip-access-list in BROADCAST-MULTICAST-CONTROL
ipv6 nd header-mismatch-validation
spanning-tree portfast
spanning-tree bpduguard enable
spanning-tree bpdufilter enable
spanning-tree mst 1 port-priority 1
spanning-tree mst 1 cost 20000
no qos trust dscp
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#

```

shutdown

[interface-config-port-channel-instance](#) on page 1059

Shutsdown this port-channel interface

Supported in the following platforms:

- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
shutdown
```

Parameters

None

Example

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#shutdown
```

Related Commands

|                                 |                                        |
|---------------------------------|----------------------------------------|
| <a href="#">no</a> on page 1065 | Re-enables this port-channel interface |
|---------------------------------|----------------------------------------|

spanning-tree

[interface-config-port-channel-instance](#) on page 1059

Configures spanning-tree related parameters on this port-channel interface

Supported in the following platforms:

- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
spanning-tree [bpdufilter|bpduguard|force-version|guard|link-type|mst|
port-cisco-interopability|portfast]
```

```
spanning-tree [bpdufilter|bpduguard] [default|disable|enable]
```

```
spanning-tree [force-version <0-3>|guard root|portfast|port-cisco-
interopability [disable|enable]]
```

```
spanning-tree link-type [point-to-point|shared]
```

```
spanning-tree mst <0-15> [cost <1-200000000>|port-priority <0-240>]]
```

Parameters

```
spanning-tree [bpdufilter|bpduguard] [default|disable|enable]
```

|                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>spanning-tree</b><br><b>[bpdufilter </b><br><b>bpduguard]</b> | <p>Configures the following BPDU related parameters for this port channel:</p> <ul style="list-style-type: none"><li>• <b>bpdufilter</b> – Configures the BPDU filtering options. The options are:<ul style="list-style-type: none"><li>• <b>default</b> – When selected, makes the bridge BPDU filter value to take effect. This is the default setting.</li><li>• <b>disable</b> – Disables BPDU filtering</li><li>• <b>enable</b> – Enables BPDU filtering. Enabling the BPDU filter feature ensures this port channel does not transmit or receive any BPDUs.</li></ul></li><li>• <b>bpduguard</b> – Configures the BPDU guard options. The options are:<ul style="list-style-type: none"><li>• <b>default</b> – When selected, makes the bridge BPDU guard value to take effect. This is the default setting.</li><li>• <b>disable</b> – Disables guarding this port from receiving BPDUs</li><li>• <b>enable</b> – Enables BPDU guarding. Enabling the BPDU guard feature means this port will shutdown on receiving a BPDU. Thus, no BPDUs are processed.</li></ul></li></ul> <p>Execute the portfast command to ensure that fast transitions is enabled on this port channel before configuring BPDU filtering and guarding.</p> |
|------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
spanning-tree [force-version <0-3>|guard root|portfast|port-cisco-interoperability
[disable|enable]]
```

|                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>spanning-tree</b><br><b>[force-version</b><br><b>&lt;0-3&gt;  guard</b><br><b>root  </b><br><b>portfast  </b><br><b>port-cisco-</b><br><b>interoperabili</b><br><b>ty [disable </b><br><b>enable]</b> | <p>Configures the following MSTP related parameters for this port channel:</p> <ul style="list-style-type: none"><li>• <b>force-version &lt;0-3&gt;</b> – Sets the protocol version to either STP(0), Not Supported(1), RSTP(2) or MSTP(3). MSTP is the default setting</li><li>• <b>guard root</b> – Enforces root bridge placement. Setting the guard to Root ensures the port is a designated port. Typically, each guard root port is a designated port, unless two or more ports (within the root bridge) are connected together.</li></ul> <p>If the bridge receives superior (BPDUs) on a guard root-enabled port, the guard root moves the port to a root-inconsistent STP state. This state is equivalent to a listening state. No data is forwarded across the port. Thus, the guard root enforces the root bridge position.</p> <ul style="list-style-type: none"><li>• <b>portfast</b> – Enables fast transitions on this port channel. When enabled, BPDU filtering and guarding can be enforced on this port. Enable the portfast option and then use the ‘bpdufilter’ and bpduguard’ options to configure BPDU filtering and guarding parameters. This option is disabled by default.</li><li>• <b>port-cisco-interoperability [disable enable]</b> – Enables or disables interoperability with Cisco’s version of MSTP, which is incompatible with standard MSTP. This option is disabled by default.</li></ul> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
spanning-tree link-type [point-to-point|shared]
```

|                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>spanning-tree link-type</b><br><b>[point-to-point   shared]</b> | Configures the link type applicable on this port channel. The options are: <ul style="list-style-type: none"> <li>point-to-point - Configures a point-to-point link, which indicates the port should be treated as connected to a point-to-point link. Note, a port connected to the wireless device is a point-to-point link. This is the default setting.</li> <li>shared - Configures a shared link, which indicates this port should be treated as having a shared connection. Note, A port connected to a hub is on a shared link.</li> </ul> |
|--------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
spanning-tree mst <0-15> [cost <1-200000000>|port-priority <0-240>]
```

|                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>spanning-tree mst &lt;0-15&gt;</b><br><b>[cost &lt;1-200000000&gt; port-priority &lt;0-240&gt;]</b> | Configures the following Multiple Spanning Tree (MST) parameters on this port: <ul style="list-style-type: none"> <li>mst &lt;0-15&gt; - Select the MST instance from 0 - 15.</li> <li>cost &lt;1-200000000&gt; - Configures the port cost from 1 - 200000000. The default path cost depends on the user defined port speed. The cost helps determine the role of the port channel in the MSTP network. The designated cost is the cost for a packet to travel from this port to the root in the MSTP configuration. The slower the media, higher the cost.</li> <li>port-priority &lt;0-240&gt; - Configures the port priority from 0 - 240. The lower the priority, greater is the likelihood of the port becoming a designated port.</li> </ul> |
|--------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Example

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#spanning-tree portfast
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#spanning-tree bpduguard enable
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#spanning-tree bpduguard enable
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#spanning-tree force-version 3
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#spanning-tree mst 1 cost 20000
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#spanning-tree mst 1 port-priority 1
```

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#show context
interface port-channel1
 description "This port-channel is for enabling dynamic LACP."
 duplex full
 ipv6 nd trust
 ipv6 nd header-mismatch-validation
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree bpduguard enable
 spanning-tree mst 1 port-priority 1
 spanning-tree mst 1 cost 20000
 ip arp trust
 port-channel load-balance src-dst-mac
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#
```

#### Related Commands

|                                 |                                                                                                              |
|---------------------------------|--------------------------------------------------------------------------------------------------------------|
| <a href="#">no</a> on page 1065 | Removes or reverts to default the spanning-tree related parameters configured on this port channel interface |
|---------------------------------|--------------------------------------------------------------------------------------------------------------|

speed

[interface-config-port-channel-instance](#) on page 1059

Configures the speed at which this port-channel interface receives and transmits data

Supported in the following platforms:

- Wireless Controllers – RFS4000



- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
speed [10|100|1000|auto]]]
```

#### Parameters

```
speed [10|100|1000|auto]
```

**speed [10|100|1000| auto]** Configure the data receive-transmit speed for this port channel. The options are:

- 10 - 10 Mbps
- 100 - 100 mbps
- 1000 - 1000 Mbps
- auto - Enables the system to auto select the speed. This is the default setting.

Select either of these options to establish a 10, 100 or 1000 Mbps data transfer rate for the selected half duplex or full duplex transmission over the port. The auto option enables the port-channel to automatically exchange information about data transmission speed and duplex capabilities. Auto negotiation is helpful in an environment where different devices are connected and disconnected on a regular basis.

#### Example

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#speed 100

nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#show context
interface port-channel1
 description "This port-channel is for enabling dynamic LACP."
 speed 100
 duplex full
 ipv6 nd trust
 ipv6 nd header-mismatch-validation
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree bpdufilter enable
 spanning-tree mst 1 port-priority 1
 spanning-tree mst 1 cost 20000
 ip arp trust
 port-channel load-balance src-dst-mac
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#
```

#### Related Commands

|                        |                                                                                                          |
|------------------------|----------------------------------------------------------------------------------------------------------|
| <b>no</b> on page 1065 | Removes or reverts to default the speed at which this port-channel interface receives and transmits data |
|------------------------|----------------------------------------------------------------------------------------------------------|

#### switchport

[interface-config-port-channel-instance](#) on page 1059

Configures the VLAN switching parameters for this port-channel interface

Supported in the following platforms:

- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
switchport [access|mode|trunk]
```

```

switchport access vlan [<1-4094>|<VLAN-ALIAS-NAME>]
switchport mode [access|trunk]
switchport trunk [allowed|native]
switchport trunk allowed vlan [<VLAN-ID>|add <VLAN-ID>|none|remove <VLAN-
ID>]
switchport trunk native [tagged|vlan [<1-4094>|<VLAN-ALIAS-NAME>]]

```

#### Parameters

```
switchport access vlan [<1-4094>|<VLAN-ALIAS-NAME>]
```

|                                                            |                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>access vlan</b><br>[<1-4094> <br><VLAN-ALIAS-<br>NAME>] | <p>Configures the VLAN to which this port-channel interface is mapped when the switching mode is set to access.</p> <ul style="list-style-type: none"> <li>• &lt;1-4094&gt; - Specify the SVI VLAN ID from 1 - 4094.</li> <li>• &lt;VLAN-ALIAS-NAME&gt; - Specify the VLAN alias name (should be existing and configured).</li> </ul> |
|------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
switchport mode [access|trunk]
```

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mode [access <br/>trunk]</b> | <p>Configures the VLAN switching mode over the port channel</p> <ul style="list-style-type: none"> <li>• access - If selected, the port channel accepts packets only from the native VLANs. Frames are forwarded out the port untagged with no 802.1Q header. All frames received on the port are expected as untagged and are mapped to the native VLAN. This is the default setting.</li> <li>• trunk - If selected, the port channel allows packets from a list of VLANs you add to the trunk. A port channel configured as Trunk supports multiple 802.1Q tagged VLANs and one Native VLAN which can be tagged or untagged.</li> </ul> |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
switchport trunk allowed vlan [<VLAN-ID>|add <VLAN-ID>|none|remove <VLAN-ID>]
```

|                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>trunk allowed</b>                                                                               | If configuring the VLAN switching mode as trunk, use this option to configure the VLANs allowed on this port channel. Add VLANs that exclusively send packets over the port channel.                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>vlan [&lt;VLAN-<br/>ID&gt;  add &lt;VLAN-<br/>ID&gt;  none <br/>remove &lt;VLAN-<br/>ID&gt;</b> | <p>Use this keyword to add/remove the allowed VLANs</p> <ul style="list-style-type: none"> <li>• &lt;VLAN-ID&gt; - Allows a group of VLAN IDs. Specify the VLAN IDs, can be either a range (55-60) or a comma-separated list (35, 41, etc.)</li> <li>• none - Allows no VLANs to transmit or receive through the layer 2 interface</li> </ul>                                                                                                                                                                                                                                                                                              |
|                                                                                                    | <ul style="list-style-type: none"> <li>• add &lt;VLAN-ID&gt; - Adds VLANs to the current list <ul style="list-style-type: none"> <li>• &lt;VLAN-ID&gt; - Specify the VLAN IDs. Can be either a range of VLAN (55-60) or a list of comma separated IDs (35, 41, etc.)</li> </ul> </li> <li>• remove &lt;VLAN-ID&gt; - Removes VLANs from the current list <ul style="list-style-type: none"> <li>• &lt;VLAN-ID&gt; - Specify the VLAN IDs. Can be either a range of VLAN (55-60) or a list of comma separated IDs (35, 41, etc.)</li> </ul> </li> </ul> <p>Allowed VLANs are configured only when the switching mode is set to "trunk".</p> |

```
switchport trunk native [tagged|vlan [<1-4094>|<VLAN-ALIAS-NAME>]]
```

|                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>trunk</b>                                                                             | If configuring the VLAN switching mode as trunk, use this option to configure the native VLAN on this port channel.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>native [tagged]  <br/>vlan [&lt;1-4094&gt;  <br/>&lt;VLAN-ALIAS-<br/>NAME&gt; ] ]</b> | <p>Configures the native VLAN ID for the trunk-mode port</p> <p>The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN untagged traffic is directed over when using a port in trunk mode.</p> <ul style="list-style-type: none"> <li>• tagged – Tags the native VLAN. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header enabling upstream Ethernet devices to know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. A native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame.</li> <li>• vlan [&lt;1-4094&gt; &lt;VLAN-ALIAS-NAME&gt;] – Sets the native VLAN for classifying untagged traffic when the interface is in trunking mode. <ul style="list-style-type: none"> <li>• &lt;1-4094&gt; – Specify a value from 1 - 4094.</li> <li>• &lt;VLAN-ALIAS-NAME&gt; – Specify the VLAN alias name used to identify the VLANs. The VLAN alias should be existing and configured.</li> </ul> </li> </ul> |

### Example

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#switchport mode trunk
```

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#show context
interface port-channel1
description "This port-channel is for enabling dynamic LACP."
speed 100
duplex full
switchport mode trunk
switchport trunk native vlan 1
no switchport trunk native tagged
switchport trunk allowed vlan 1
ipv6 nd trust
ipv6 nd header-mismatch-validation
spanning-tree portfast
spanning-tree bpduguard enable
spanning-tree bpdufilter enable
spanning-tree mst 1 port-priority 1
spanning-tree mst 1 cost 20000
ip arp trust
port-channel load-balance src-dst-mac
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#
```

### Related Commands

|                        |                                                                                   |
|------------------------|-----------------------------------------------------------------------------------|
| <b>no</b> on page 1065 | Removes the packet switching parameters configured on this port-channel interface |
|------------------------|-----------------------------------------------------------------------------------|

use

[interface-config-port-channel-instance](#) on page 1059

Configures access controls on this port-channel interface

Supported in the following platforms:

- Wireless Controllers – RFS4000
- Service Platforms – NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

## Syntax

```
use [ip-access-list|ipv6-access-list|mac-access-list] in <IP/IPv6/MAC-ACCESS-LIST-NAME>]]
```

## Parameters

```
use [ip-access-list|ipv6-access-list|mac-access-list] in <IP/IPv6/MAC-ACCESS-LIST-NAME>]
```

|                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre><b>use [ip-<br/>access-list  <br/>ipv6-access-<br/>list   mac-<br/>access-list]<br/>&lt;IP/IPv6/MAC-<br/>ACCESS-LIST-<br/>NAME&gt; ]</b></pre> | <p>Associates an access list controlling the inbound traffic on this port channel.</p> <ul style="list-style-type: none"><li>• ip-access-list – Specify the IPv4 specific firewall rules to apply to this profile's port channel configuration. IPv4 is a connectionless protocol for packet switched networking. IPv4 operates as a best effort delivery method, as it does not guarantee delivery, and does not ensure proper sequencing or duplicate delivery (unlike (TCP). IPv4 hosts can use link local addressing to provide local connectivity.</li><li>• ipv6-access-list – Specify the IPv6 specific firewall rules to apply to this profile's port channel configuration. IPv6 is the latest revision of the Internet Protocol (IP) designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.</li><li>• mac-access-list – Specify the MAC specific firewall rules to apply to this profile's port channel configuration.</li><li>• &lt;IP/IPv6/MAC-ACCESS-LIST-NAME&gt; – Provide the IPv4, IPv6, or MAC access list name based on the option selected. The access list specified should be existing and configured.</li></ul> |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Example

```
nx9500-6C8809(config-profile-testNX9000-if-port-channell)#use ip-access-list in
BROADCAST-MULTICAST-CONTROL
```

```
nx9500-6C8809(config-profile-testNX9000-if-port-channell)#show context
interface port-channell
description "This port-channel is for enabling dynamic LACP."
speed 100
duplex full
switchport mode trunk
switchport trunk native vlan 1
no switchport trunk native tagged
switchport trunk allowed vlan 1
use ip-access-list in BROADCAST-MULTICAST-CONTROL
ipv6 nd trust
ipv6 nd header-mismatch-validation
spanning-tree portfast
--More--
nx9500-6C8809(config-profile-testNX9000-if-port-channell)#
```

## Related Commands

|                                 |                                                                       |
|---------------------------------|-----------------------------------------------------------------------|
| <a href="#">no</a> on page 1065 | Removes the access controls configured on this port-channel interface |
|---------------------------------|-----------------------------------------------------------------------|

## interface-config-radio-instance

[interface](#) on page 1013

This section documents radio interface configuration parameters applicable only to the access point profiles.

The access point radio interface can be radio1, radio2, or radio3. The AP7662 model is a dual radio access point. Whereas, AP8533 is a triple radio access point.

To enter the AP profile > radio interface context, use the following commands:

```
<DEVICE>(config)#profile <AP-TYPE> <PROFILE-NAME>
```

```
nx9500-6C8809(config)#profile ap7532 test7532
nx9500-6C8809(config-profile-test7532)#
```

```
nx9500-6C8809(config-profile-test7532)#interface radio 2
nx9500-6C8809(config-profile-test7532-if-radio2)#
```

```
nx9500-6C8809(config-profile-test7532-if-radio2)#?
```

Radio Mode commands:

|                            |                                                                                                                         |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------|
| adaptivity                 | Adaptivity                                                                                                              |
| aer scout                  | Aer scout Multicast MAC/Enable                                                                                          |
| aggregation                | Configure 802.11n aggregation related parameters                                                                        |
| airtime-fairness           | Enable fair access to medium for clients based on their usage of airtime                                                |
| antenna-diversity          | Transmit antenna diversity for non-11n transmit rates                                                                   |
| antenna-downtilt           | Enable ADEPT antenna mode                                                                                               |
| antenna-elevation          | Specifies the antenna elevation gain                                                                                    |
| antenna-gain               | Specifies the antenna gain of this radio                                                                                |
| antenna-mode               | Configure the antenna mode (number of transmit and receive antennas) on the radio                                       |
| assoc-response             | Configure transmission parameters for Association Response frames                                                       |
| association-list           | Configure the association list for the radio                                                                            |
| beacon                     | Configure beacon parameters                                                                                             |
| bridge                     | Bridge rf-mode related configuration                                                                                    |
| channel                    | Configure the channel of operation for this radio                                                                       |
| data-rates                 | Specify the 802.11 rates to be supported on this radio                                                                  |
| description                | Configure a description for this radio                                                                                  |
| dfs-rehome                 | Revert to configured home channel once dfs evacuation period expires                                                    |
| dynamic-chain-selection    | Automatic antenna-mode selection (antenna for non-11n transmit rates)                                                   |
| ekahau                     | Ekahau Multicast MAC/Enable                                                                                             |
| extended-range             | Configure extended range                                                                                                |
| fallback-channel           | Configure the channel to be used for falling back in the event of radar being detected on the current operating channel |
| guard-interval             | Configure the 802.11n guard interval                                                                                    |
| ldpc                       | Configure support for Low Density Parity Check Code                                                                     |
| lock-rf-mode               | Retain user configured rf-mode setting for this radio                                                                   |
| max-clients                | Maximum number of wireless clients allowed to associate subject to AP limit                                             |
| mesh                       | Configure radio mesh parameters                                                                                         |
| meshpoint                  | Enable meshpoints on this radio                                                                                         |
| mu-mimo                    | Enable multi user MIMO on this radio (selected platforms only)                                                          |
| no                         | Negate a command or set its defaults                                                                                    |
| non-unicast                | Configure handling of non-unicast frames                                                                                |
| off-channel-scan           | Enable off-channel scanning on the radio                                                                                |
| placement                  | Configure the location where this radio is operating                                                                    |
| power                      | Configure the transmit power of the radio                                                                               |
| preamble-short             | Use short preambles on this radio                                                                                       |
| probe-response             | Configure transmission parameters for Probe Response frames                                                             |
| radio-resource-measurement | Configure support for 802.11k Radio Resource Measurement                                                                |

```

radio-share-mode Configure the radio-share mode of operation for
 this radio
rate-selection Default or Opportunistic rate relection
rf-mode Configure the rf-mode of operation for this
 radio
rifs Configure Reduced Interframe Spacing (RIFS)
 parameters
rts-threshold Configure the RTS threshold
shutdown Shutdown the selected radio interface
smart-rf Configure radio specific smart-rf settings
sniffer-redirect Capture packets and redirect to an IP address
 running a packet capture/analysis tool
stbc Configure Space-Time Block Coding (STBC)
 parameters
transmit-beamforming Enable Transmit Beamforming
use Set setting to use
wips Wireless intrusion prevention related
 configuration
wireless-client Configure wireless client related parameters
wlan Enable wlans on this radio

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or
 terminal

```

```
nx9500-6C8809(config-profile-test7532-if-radio2)#
```

The following table summarizes the radio interface configuration commands:

| Commands                                       | Description                                                                                                                      |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">adaptivity</a> on page 1076        | Configures an adaptivity timeout value, in minutes, for avoidance of channels detected with radar or high levels of interference |
| <a href="#">aeroscout</a> on page 1077         | Enables Aeroscout multicast packet forwarding                                                                                    |
| <a href="#">aggregation</a> on page 1078       | Configures 802.11n aggregation parameters                                                                                        |
| <a href="#">airtime-fairness</a> on page 1081  | Enables fair access for clients based on airtime usage                                                                           |
| <a href="#">antenna-diversity</a> on page 1081 | Transmits antenna diversity for non-11n transmit rates                                                                           |
| <a href="#">antenna-downtilt</a> on page 1082  | Enables Advanced Element Panel Technology (ADEPT) antenna mode                                                                   |
| <a href="#">antenna-elevation</a> on page 1082 | Configures the antenna's elevation gain. This command is applicable only to the AP7562 model access point.                       |
| <a href="#">antenna-gain</a> on page 1084      | Specifies the antenna gain for the selected radio                                                                                |

| Commands                                             | Description                                                                                                                                                                            |
|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">antenna-mode</a> on page 1085            | Configures the radio antenna mode                                                                                                                                                      |
| <a href="#">assoc-response</a> on page 1086          | Enables an access point to ignore or respond to an association/authorization request based on the configured Received Signal Strength Index (RSSI) threshold and deny-threshold values |
| <a href="#">association-list</a> on page 1086        | Associates an existing global association list with this radio interface                                                                                                               |
| <a href="#">beacon</a> on page 1087                  | Configures beacon parameters                                                                                                                                                           |
| <a href="#">bridge</a> on page 1088                  | Configures client-bridge related parameters, if the selected radio's RF mode is set to bridge                                                                                          |
| <a href="#">channel</a> on page 1098                 | Configures a radio's channel of operation                                                                                                                                              |
| <a href="#">data-rates</a> on page 1099              | Specifies the 802.11 rates supported on a radio                                                                                                                                        |
| <a href="#">description</a> on page 1103             | Configures the selected radio's description                                                                                                                                            |
| <a href="#">dfs-rehome</a> on page 1104              | Reverts to configured home channel once Dynamic Frequency Selection (DFS) evacuation period expires                                                                                    |
| <a href="#">dynamic-chain-selection</a> on page 1105 | Enables automatic antenna mode selection                                                                                                                                               |
| <a href="#">ekahau</a> on page 1105                  | Enables Ekahau multicast packet forwarding                                                                                                                                             |
| <a href="#">extended-range</a> on page 1106          | Configures extended range                                                                                                                                                              |
| <a href="#">fallback-channel</a> on page 1107        | Configures the channel to which the radio switches in case of radar detection on the current channel                                                                                   |
| <a href="#">guard-interval</a> on page 1108          | Configures the 802.11n guard interval                                                                                                                                                  |
| <a href="#">ldpc</a> on page 1109                    | Enables support for Low Density Parity Check (LDPC) on the radio interface                                                                                                             |
| <a href="#">lock-rf-mode</a> on page 1110            | Retains user configured RF mode settings for the selected radio                                                                                                                        |
| <a href="#">max-clients</a> on page 1111             | Configures the maximum number of wireless clients allowed to associate with this radio                                                                                                 |
| <a href="#">mesh</a> on page 1112                    | Configures radio mesh parameters                                                                                                                                                       |
| <a href="#">meshpoint</a> on page 1113               | Maps an existing meshpoint to this radio interface                                                                                                                                     |
| <a href="#">mu-mimo</a> on page 1113                 | Enables multi-user multiple input multiple output (MU-MIMO) support on a radio                                                                                                         |
| <a href="#">no</a> on page 1114                      | Negates or resets radio interface settings configured on a profile or a device                                                                                                         |
| <a href="#">non-unicast</a> on page 1117             | Configures the handling of non unicast frames on this radio                                                                                                                            |
| <a href="#">off-channel-scan</a> on page 1119        | Enables selected radio's off channel scanning parameters                                                                                                                               |

| Commands                                                | Description                                                                                                                       |
|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">placement</a> on page 1120                  | Defines selected radio's deployment location                                                                                      |
| <a href="#">power</a> on page 1121                      | Configures the transmit power on this radio                                                                                       |
| <a href="#">preamble-short</a> on page 1122             | Enables the use of short preamble on this radio                                                                                   |
| <a href="#">probe-response</a> on page 1123             | Configures transmission parameters for probe response frames                                                                      |
| <a href="#">radio-resource-measurement</a> on page 1124 | Enables 802.11k radio resource measurement                                                                                        |
| <a href="#">radio-share-mode</a> on page 1125           | Configures the mode of operation, for this radio, as radio-share                                                                  |
| <a href="#">rate-selection</a> on page 1126             | Sets the rate selection method to standard or opportunistic                                                                       |
| <a href="#">rf-mode</a> on page 1127                    | Configures the radio's RF mode                                                                                                    |
| <a href="#">rifs</a> on page 1129                       | Configures Reduced Interframe Spacing (RIFS) parameters on this radio                                                             |
| <a href="#">rts-threshold</a> on page 1129              | Configures the Request to Send (RTS) threshold value on this radio                                                                |
| <a href="#">service</a> on page 1130                    | Enables dynamic control function. This dynamic function controls performance of the radio receiver's low noise amplifiers (LNAs). |
| <a href="#">shutdown</a> on page 1131                   | Terminates or shuts down selected radio interface                                                                                 |
| <a href="#">smart-rf</a> on page 1132                   | Overrides Smart RF channel width setting on the selected radio interface                                                          |
| <a href="#">sniffer-redirect</a> on page 1132           | Captures and redirects packets to an IP address running a packet capture/analysis tool                                            |
| <a href="#">stbc</a> on page 1133                       | Configures radio's Space Time Block Coding (STBC) mode                                                                            |
| <a href="#">transmit-beamforming</a> on page 1134       | Enables transmit beamforming on the selected radio interface                                                                      |
| <a href="#">use</a> on page 1135                        | Enables use of an association ACL policy and a radio QoS policy by selected radio interface                                       |
| <a href="#">wips</a> on page 1136                       | Enables access point to change its channel of operation in order to terminate rogue devices                                       |
| <a href="#">wireless-client</a> on page 1137            | Configures wireless client parameters on selected radio                                                                           |
| <a href="#">wlan</a> on page 1138                       | Enables a WLAN on selected radio                                                                                                  |

adaptivity

[interface-config-radio-instance](#) on page 1072

Configures the duration, in minutes, for which channels detected with high levels of interference are avoided by the AP



As per the ETSI's (European Telecommunications Standards Institute) EN 300 328 V1.8.1/ ETSI EN 301 893 V1.7.1 requirements, access points have to monitor interference levels on operating channels, and stop functioning on channels with interference levels exceeding ETSI-specified threshold values.

This command configures the duration for which a channel is avoided on detection of interference, and is applicable only if the channel selection mode is set to ACS, Random, or Fixed.



#### Note

If you want to configure your radio to use a SMART RF policy for channel selection (i.e., the radio's channel selection mode is set to Smart), in the Smart-RF policy config mode, use the **avoidance-time > [adaptivity|dfs] > <30-3600>** command to specify the interval for which a channel is avoided on detection of high levels of interference or radar. For more information, see [avoidance-time](#) on page 1633 (smart-rf policy config mode).

When configured, this feature ensures recovery by switching the radio to a new operating channel. Once adaptivity is triggered, the evacuated channel becomes inaccessible and is available again only after the adaptivity timeout, specified here, expires. In case of fixed channel, the radio switches back to the original channel of operation after the adaptivity timeout expires. On the other hand, ACS-enabled radios continue operating on the new channel even after the adaptivity timeout period expires.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

#### Syntax

```
adaptivity [recovery|timeout <30-3600>]
```

#### Parameters

```
adaptivity [recovery|timeout <30-3600>]
```

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>adaptivity</b>                        | Configures adaptivity parameters on the radio. These parameters are: recovery and timeout.                                                                                                                                                                                                                                                                                                                  |
| <b>recovery</b>                          | Enables switching of channels when an access point's radio is in the adaptivity mode. In the adaptivity mode, an access point monitors interference on its set channel and stops functioning when the radio's defined interference tolerance level is exceeded. When the defined adaptivity timeout is exceeded, the radio resumes functionality on a different channel. This option is enabled by default. |
| <b>timeout</b><br><b>&lt;30-3600&gt;</b> | Configures an adaptivity timeout <ul style="list-style-type: none"><li>• &lt;30-3600&gt; – Specify a value from 30 - 3600 minutes. The default is 90 minutes.</li></ul>                                                                                                                                                                                                                                     |

#### Example

```
nx9500-6C8809(config-profile-testAP7532-if-radiol)#adaptivity timeout 200
```

```
nx9500-6C8809(config-profile-testAP7532-if-radiol)#show context
 interface radiol
 adaptivity timeout 200
nx9500-6C8809(config-profile-testAP7532-if-radiol)#
```

#### Related Commands

|                                 |                                                                                  |
|---------------------------------|----------------------------------------------------------------------------------|
| <a href="#">no</a> on page 1114 | Removes the configured adaptivity timeout value and disables adaptivity recovery |
|---------------------------------|----------------------------------------------------------------------------------|

aeroscout

[interface-config-radio-instance](#) on page 1072

Enables Aeroscout multicast packet forwarding. This feature is disabled by default.

Supported in the following platforms:

- Access Points — AP7502, AP7522

Syntax

```
aeroscout [forward ip <IP> port <0-65535>|mac <MAC>]
```

Parameters

```
aeroscout [forward ip <IP> port <0-65535>|mac <MAC>]
```

|                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>aeroscout</b>                                          | Enables Aeroscout packet forwarding and configures the packet forwarding parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>forward ip<br/>&lt;IP&gt; port<br/>&lt;0-65535&gt;</b> | Configures the following Aeroscout locationing engine details: <ul style="list-style-type: none"><li>• ip - Configures Aeroscout engine's IP address<ul style="list-style-type: none"><li>• &lt;IP&gt; - Specify the Aeroscout engine's IP address. When specified, the AP forwards Aeroscout beacons directly to the Aeroscout locationing engine without proxying through the controller or RF Domain manager.</li></ul></li><li>• port - Configures the port on which the Aeroscout engine is reachable<ul style="list-style-type: none"><li>• &lt;0-65535&gt; - Specify the port number from 0 - 65535.</li></ul></li></ul> |
| <b>mac &lt;MAC&gt;</b>                                    | Configures the multicast MAC address to forward the Aeroscout packets <ul style="list-style-type: none"><li>• &lt;MAC&gt; - Specify the MAC address in the AA-BB-CC-DD-EE-FF format. The default value is 01-0C-CC-00-00-00.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                          |

Example

```
nx9500-6C8809(config-profile-ProfileTestAP7532-if-radio2)#aeroscout forward ip
10.233.84.206 port 22
```

```
nx9500-6C8809(config-profile-ProfileTestAP7532-if-radio2)#show context
interface radio2
aeroscout forward ip 10.233.84.206 port 22
nx9500-6C8809(config-profile-ProfileTestAP7532-if-radio2)#
```

Related Commands

|                                 |                                      |
|---------------------------------|--------------------------------------|
| <a href="#">no</a> on page 1114 | Disables Aeroscout packet forwarding |
|---------------------------------|--------------------------------------|

aggregation

[interface-config-radio-instance](#) on page 1072

Configures 802.11n frame aggregation parameters. Frame aggregation increases throughput by sending two or more data frames in a single transmission. There are two types of frame aggregation: MAC Service Data Unit (MSDU) aggregation and MAC Protocol Data Unit (MPDU) aggregation. Both modes group several data frames into one large data frame.

Supported in the following platforms:

- Access Points — AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

Syntax

```
aggregation [ampdu|amsdu]
```

```
aggregation ampdu [rx-only|tx-only|tx-rx|none|max-aggr-size|min-spacing]
```

```
aggregation ampdu [rx-only|tx-only|tx-rx|none]
```

```
aggregation ampdu max-aggr-size [rx|tx]
```

```
aggregation ampdu max-aggr-size rx [8191|16383|32767|65535]
```

```
aggregation ampdu max-aggr-size tx <2000-65535>
```

```
aggregation ampdu min-spacing [0|1|2|4|8|16]
```

```
aggregation amsdu [rx-only|tx-rx]
```

Parameters

```
aggregation ampdu [rx-only|tx-only|tx-rx|none]
```

|                    |                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>aggregation</b> | Configures 802.11n frame aggregation parameters                                                                                                                                                                                                                                                                                                                                                               |
| <b>ampdu</b>       | Configures Aggregate MAC Protocol Data Unit (AMPDU) frame aggregation parameters. AMPDU aggregation collects Ethernet frames addressed to a single destination. It wraps each frame in an 802.11n MAC header. This aggregation mode is less efficient, but more reliable in environments with high error rates. It enables the acknowledgement and retransmission of each aggregated data frame individually. |
| <b>tx-only</b>     | Supports the transmission of AMPDU aggregated frames only                                                                                                                                                                                                                                                                                                                                                     |
| <b>rx-only</b>     | Supports the receipt of AMPDU aggregated frames only                                                                                                                                                                                                                                                                                                                                                          |
| <b>tx-rx</b>       | Supports the transmission and receipt of AMPDU aggregated frames (default setting)                                                                                                                                                                                                                                                                                                                            |
| <b>none</b>        | Disables support for AMPDU aggregation                                                                                                                                                                                                                                                                                                                                                                        |

```
aggregation ampdu max-aggr-size rx [8191|16383|32767|65535]
```

|                                    |                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>aggregation</b>                 | Configures 802.11n frame aggregation parameters                                                                                                                                                                                                                                                                                                                            |
| <b>ampdu</b>                       | Configures AMPDU frame aggregation parameters. AMPDU aggregation collects Ethernet frames addressed to a single destination. It wraps each frame in an 802.11n MAC header. This aggregation mode is less efficient, but more reliable in environments with high error rates. It enables the acknowledgement and retransmission of each aggregated data frame individually. |
| <b>max-aggr-size</b>               | Configures AMPDU packet size limits. Configure the packet size limit for transmitted and received packets.                                                                                                                                                                                                                                                                 |
| <b>rx [8191 16383 32767 65535]</b> | Configures the maximum limit (in bytes) advertised for received frames <ul style="list-style-type: none"><li>• 8191 – Advertises a maximum of 8191 bytes</li><li>• 16383 – Advertises a maximum of 16383 bytes</li><li>• 32767 – Advertises a maximum of 32767 bytes</li><li>• 65535 – Advertises a maximum of 65535 bytes (default setting)</li></ul>                     |

```
aggregation ampdu max-aggr-size tx <2000-65535>
```

|                              |                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>aggregation</b>           | Configures 802.11n frame aggregation parameters                                                                                                                                                                                                                                                                                                                              |
| <b>ampdu</b>                 | Configures AMPDU frame aggregation parameters<br>AMPDU aggregation collects Ethernet frames addressed to a single destination. It wraps each frame in an 802.11n MAC header. This aggregation mode is less efficient, but more reliable in environments with high error rates. It enables the acknowledgement and retransmission of each aggregated data frame individually. |
| <b>max-aggr-size</b>         | Configures AMPDU packet size limits. Configure the packet size limit for transmitted and received packets.                                                                                                                                                                                                                                                                   |
| <b>tx &lt;2000-65535&gt;</b> | Configures the maximum size (in bytes) for AMPDU aggregated transmitted frames <ul style="list-style-type: none"> <li>&lt;2000-65535&gt; - Sets the limit from 2000 - 65535 bytes. The default is 65535 bytes.</li> </ul>                                                                                                                                                    |

```
aggregation ampdu min-spacing [0|1|2|4|8|16|auto]
```

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>aggregation</b>                | Configures 802.11n frame aggregation parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>ampdu</b>                      | Configures AMPDU frame aggregation parameters<br>AMPDU aggregation collects Ethernet frames addressed to a single destination. It wraps each frame in an 802.11n MAC header. This aggregation mode is less efficient, but more reliable in environments with high error rates. It enables the acknowledgement and retransmission of each aggregated data frame individually.                                                                                                                                                                                                        |
| <b>min-spacing [0 1 2 4 8 16]</b> | Configures the minimum gap, in microseconds, between AMPDU frames <ul style="list-style-type: none"> <li>0 - Configures the minimum gap as 0 microseconds</li> <li>1 - Configures the minimum gap as 1 microseconds</li> <li>2 - Configures the minimum gap as 2 microseconds</li> <li>4 - Configures the minimum gap as 4 microseconds</li> <li>8 - Configures the minimum gap as 8 microseconds</li> <li>16 - Configures the minimum gap as 16 microseconds</li> <li>auto - Auto configures the minimum gap depending on the platform and radio type (default setting)</li> </ul> |

```
aggregation amsdu [rx-only|tx-rx]
```

|                    |                                                                                                                                                                                                                                   |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>aggregation</b> | Configures 802.11n frame aggregation parameters                                                                                                                                                                                   |
| <b>amsdu</b>       | Configures Aggregated MAC Service Data Unit (AMSDU) frame aggregation parameters. AMSDU aggregation collects Ethernet frames addressed to a single destination. But, unlike AMPDU, it wraps all frames in a single 802.11n frame. |
| <b>rx-only</b>     | Supports the receipt of AMSDU aggregated frames only (default setting)                                                                                                                                                            |
| <b>tx-rx</b>       | Supports the transmission and receipt of AMSDU aggregated frames                                                                                                                                                                  |

#### Example

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radio1)#aggregation ampdu tx-only
```

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radio1)#show context
interface radio1
 aggregation ampdu tx-only
 aeroscout forward
nx9500-6C8809(config-profile-7lxxTestProfile-if-radio1)#
```

#### Related Commands

|                        |                                         |
|------------------------|-----------------------------------------|
| <b>no</b> on page 1114 | Disables 802.11n aggregation parameters |
|------------------------|-----------------------------------------|

## airtime-fairness

[interface-config-radio-instance](#) on page 1072

Enables fair access to the medium for wireless clients based on their airtime usage, regardless of whether the client is a high-throughput (802.11n) or legacy client. This option is enabled by default.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

Syntax

```
airtime-fairness {prefer-ht} {weight <1-10>}
```

Parameters

```
airtime-fairness {prefer-ht} {weight <1-10>}
```

|                            |                                                                                                                                                                                                      |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>airtime-fairness</b>    | Enables fair access to the medium for wireless clients based on their airtime usage                                                                                                                  |
| <b>prefer-ht</b>           | Optional. Prioritizes high throughput (802.11n) clients over clients with slower throughput (802.11 a/b/g) and legacy clients                                                                        |
| <b>weight &lt;1-10&gt;</b> | Optional. Configures the relative weightage for 11n clients over legacy clients. <ul style="list-style-type: none"><li>• &lt;1-10&gt; - Sets a weightage ratio for 11n clients from 1 - 10</li></ul> |

Example

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radio1)#airtime-fairness prefer-ht weight 6
```

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radio1)#show context
interface radio1
 aggregation ampdu tx-only
 aeroscout forward
 airtime-fairness prefer-ht weight 6
nx9500-6C8809(config-profile-7lxxTestProfile-if-radio1)#
```

Related Commands

|                                 |                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------|
| <a href="#">no</a> on page 1056 | Disables fair access for wireless clients (provides access on a round-robin mode) |
|---------------------------------|-----------------------------------------------------------------------------------|

## antenna-diversity

[interface-config-radio-instance](#) on page 1072

Enables antenna diversity for transmit frames at non-11n transmit rates

Antenna diversity uses two or more antennas to increase signal quality and strength. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

Syntax

```
antenna-diversity
```

Parameters

None

#### Example

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radio1)#antenna-diversity
```

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radio1)#show context
 interface radio1
 aggregation ampdu tx-only
 aeroscout forward
 antenna-diversity
 airtime-fairness prefer-ht weight 6
nx9500-6C8809(config-profile-7lxxTestProfile-if-radio1)#
```

#### Related Commands

|                                 |                                                |
|---------------------------------|------------------------------------------------|
| <a href="#">no</a> on page 1114 | Uses single antenna for non-11n transmit rates |
|---------------------------------|------------------------------------------------|

### antenna-downtilt

[interface-config-radio-instance](#) on page 1072

Enables the Advanced Element Panel Technology (ADEPT) antenna mode. The ADEPT mode increases the probability of parallel data paths enabling multiple spatial data streams. This option is disabled by default.

Supported in the following platforms:

- Access Point — AP7161

#### Syntax

```
antenna-downtilt
```

#### Parameters

None

#### Example

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radio1)#antenna-downtilt
```

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radio1)#show context
 interface radio1
 antenna-gain 12.0
 aggregation ampdu tx-only
 aeroscout forward
 antenna-diversity
 airtime-fairness prefer-ht weight 6
 antenna-downtilt
nx9500-6C8809(config-profile-7lxxTestProfile-if-radio1)#
```

#### Related Commands

|                                 |                                 |
|---------------------------------|---------------------------------|
| <a href="#">no</a> on page 1114 | Disables the ADEPT antenna mode |
|---------------------------------|---------------------------------|

### antenna-elevation

[interface-config-radio-instance](#) on page 1072

Configures an antenna's elevation gain. Antenna gain is the ratio of an antenna's radiation intensity in a given direction to the intensity produced by a no-loss, isotropic antenna radiating equally in all directions. An antenna's gain along the horizon and at an elevation of 30 degree may vary. The elevation

gain is defined as the maximum antenna gain at 30 to 150 degrees above the horizon. If elevation gain is configured, the transmit (TX) power calculations maximize the allowable TX power for an elevation below 30 degree.

Access points must conform to U.S. Federal Communications Commission's (FCC) limitations. FCC has now stipulated a 21dBm Effective Isotropic Radiated Power (EIRP) limit for power directed 30 degrees above the horizon.

For Extreme Networks -supplied antennas, compatible with 5.0 GHz on the AP7562 access point, refer to the Antenna Guide for "Elevation Gain" information. If using a third-party antenna, it is required that you obtain the antenna-elevation gain information from the antenna manufacturer.

The elevation gain should be configured if the access point:

- Is deployed outdoors, and
- Is used with a dipole antenna (panel antenna and polarized antenna are for point to point only, and are excluded from this requirement), and
- Is transmitting in the 5.15 - 5.25 GHz Unlicensed National Information Infrastructure-1 (UNII-1) band.

Professional installers must complete the following steps to ensure compliance with the FCC rule:

- 1 Configure the antenna type. For example:  
`ap7562-80C2AC(config-device-84-24-8D-80-C2-AC-if-radio2)#service antenna-type dipole`
- 2 Configure the antenna peak gain. For example:  
`ap7562-80C2AC(config-device-84-24-8D-80-C2-AC-if-radio2)#antenna-gain 7.0`
- 3 Configure the antenna placement. For example:  
`ap7562-80C2AC(config-device-84-24-8D-80-C2-AC-if-radio2)#placement outdoor`
- 4 Configure the antenna elevation gain. For example:  
`ap7562-80C2AC(config-device-84-24-8D-80-C2-AC-if-radio2)#antenna-elevation 5.0`

After the professional installer enters the antenna type, gain, placement, and elevation gain using the CLI as outlined above, the firmware will use this information and hardcoded maximum limits determined during testing (See Annex C in FCC Report #FR4D0448AB) to limit the EIRP below 21dBm for outdoor use in UNII-1 band. The antenna information is provided in the Installation guide and antenna guide.

Supported in the following platforms:

- Access Points — AP7562

Syntax

`antenna-elevation <-30.0-36.0>`



#### Note

The antenna elevation gain feature is supported only on the AP7562 model access point.

Parameters

`antenna-elevation <-30.0-36.0>`

|                                                       |                                                                                                                                                                       |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>antenna-elevation</b><br><b>&lt;-30.0-36.0&gt;</b> | Configures the antenna elevation gain from -30.0 - 36.0 dB. Refer to the antenna specifications for antenna-elevation gain information.<br>The default value is 0 dB. |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Example

```
ap7562-80C2AC(config-device-84-24-8D-80-C2-AC-if-radio2)#antenna-elevation 5.0

ap7562-80C2AC(config-device-84-24-8D-80-C2-AC-if-radio2)#show context
interface radio2
 antenna-elevation 5.0
ap7562-80C2AC(config-device-84-24-8D-80-C2-AC-if-radio2)#
```

## Related Commands

|                                 |                                                 |
|---------------------------------|-------------------------------------------------|
| <a href="#">no</a> on page 1114 | Resets antenna elevation gain to default (0 dB) |
|---------------------------------|-------------------------------------------------|

## antenna-gain

[interface-config-radio-instance](#) on page 1072

Configures the antenna gain for the selected radio

Antenna gain is the ability of an antenna to convert power into radio waves and vice versa. The access point or wireless controller's Power Management Antenna Configuration File (PMACF) automatically configures the access point or wireless controller's radio transmit power based on the antenna type, its antenna gain (provided here) and the deployed country's regulatory domain restrictions. Once provided, the access point or wireless controller calculates the power range. Antenna gain relates the intensity of an antenna in a given direction to the intensity that would be produced ideally by an antenna that radiates equally in all directions (isotropically), and has no losses. Although the gain of an antenna is directly related to its directivity, its gain is a measure that takes into account the efficiency of the antenna as well as its directional capabilities. It is recommended that only a professional installer set the antenna gain.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

## Syntax

```
antenna-gain <0.0-15.0>
```

## Parameters

```
antenna-gain <0.0-15.0>
```

|                                                |                                                                     |
|------------------------------------------------|---------------------------------------------------------------------|
| <b>antenna-gain</b><br><b>&lt;0.0-15.0&gt;</b> | Sets the antenna gain from 0.0 - 15.0 dBi. The default is 0.00 dBi. |
|------------------------------------------------|---------------------------------------------------------------------|

## Example

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radio1)#antenna-gain 12.0

nx9500-6C8809(config-profile-71xxTestProfile-if-radio1)#show context
interface radio1
 antenna-gain 12.0
 aggregation ampdu tx-only
 aeroscout forward
 antenna-diversity
 airtime-fairness prefer-ht weight 6
 antenna-downtilt
nx9500-6C8809(config-profile-71xxTestProfile-if-radio1)#
```

## Related Commands



[no](#) on page 1114

Resets the radio's antenna gain parameter

## antenna-mode

[interface-config-radio-instance](#) on page 1072

Configures the antenna mode (the number of transmit and receive antennas) on the access point

This command sets the number of transmit and receive antennas on the access point. The 1x1 mode is used for transmissions over just the single -A- antenna, 1xALL is used for transmissions over the -A- antenna and all three antennas for receiving. The 2x2 mode is used for transmissions and receipts over two antennas for dual antenna models. 3x3x3 is used for transmissions and receipts over three antennas for AP8163 models. The default setting is dynamic based on the access point model deployed and its transmit power settings.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

### Syntax

```
antenna-mode [1*1|1*ALL|2*2|3*3|default]
```

### Parameters

```
antenna-mode [1*1|1*ALL|2*2|default]
```

|                     |                                                             |
|---------------------|-------------------------------------------------------------|
| <b>antenna-mode</b> | Configures the antenna mode                                 |
| <b>1*1</b>          | Uses only antenna A to receive and transmit                 |
| <b>1*ALL</b>        | Uses antenna A to transmit and receives on all antennas     |
| <b>2*2</b>          | Uses antennas A and C for both transmit and receive         |
| <b>3*3</b>          | Uses antenna A, B, and C for both transmit and receive      |
| <b>default</b>      | Uses default antenna settings. This is the default setting. |

### Usage Guidelines

To support STBC feature on AP7161 profile, the antenna-mode should not be configured to 1\*1.

### Example

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radio1)#antenna-mode 2x2
```

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radio1)#show context
```

```
interface radio1
 antenna-gain 12.0
 aggregation ampdu tx-only
 aeroscout forward
 antenna-mode 2x2
 antenna-diversity
 airtime-fairness prefer-ht weight 6
 antenna-downtilt
```

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radio1)#
```

### Related Commands

[no](#) on page 1114

Resets the radio antenna mode (the number of transmit and receive antennas) to its default

assoc-response

[interface-config-radio-instance](#) on page 1072

Configures the parameters determining whether the access point ignores or responds to an association/authorization request

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

Syntax

```
assoc-response [deny-threshold <1-12>|rssi-threshold <-128--40>]
```

Parameters

```
assoc-response [deny-threshold <1-12>|rssi-threshold <-128--40>]
```

|                                                  |                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>assoc-response</b>                            | Configures the following thresholds, based on which the AP ignores or responds to an association/authorization request: deny-threshold and rssi-threshold. Both these options are disabled by default.                                                                                                                                                                                      |
| <b>deny-threshold</b><br><b>&lt;1-12&gt;</b>     | Configures the number of times the AP ignores association/authorization requests, if the RSSI is below the configured RSSI threshold value <ul style="list-style-type: none"><li>• &lt;1-12&gt; - Specify a value from 1 - 12.</li></ul> <p><b>Note:</b> The AP always ignores association/authorization requests when deny-threshold is not specified and rssi-threshold is specified.</p> |
| <b>rssi-threshold</b><br><b>&lt;-128--40&gt;</b> | Configures the RSSI threshold. If the RSSI is lower than the threshold configured here, the AP ignores the association/authorization request. <ul style="list-style-type: none"><li>• &lt;128--40&gt; - Specify the RSSI threshold from -128 - -40 dBi.</li></ul>                                                                                                                           |

Example

```
nx9500-6C8809(config-profile-71XXTestProfile-if-radio1)#assoc-response rssi-threshold -128
```

```
nx9500-6C8809(config-profile-71XXTestProfile-if-radio1)#show context
 interface radio1
 assoc-response rssi-threshold -128
nx9500-6C8809(config-profile-71XXTestProfile-if-radio1)#
```

Related Commands

|                                 |                                                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------|
| <a href="#">no</a> on page 1114 | Removes the RSSI threshold, based on which an association/authorization request is either ignored or responded. |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------|

association-list

[interface-config-radio-instance](#) on page 1072

Associates an existing global association list with this radio interface

An association ACL is a policy-based access control list (ACL) that either prevents or allows wireless clients from connecting to a managed access point radio. An ACL is a sequential collection of permit and deny rules that apply to incoming and outgoing packets. When a packet is received on an interface, the controller, service platform, or access point compares the fields in the packet against the applied

ACLs to verify the packet has the required permissions to be forwarded. If a packet does not meet any of the criteria specified in the ACL, it is dropped.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

Syntax

```
association-list global <GLOBAL-ASSOC-LIST-NAME>
```

Parameters

```
association-list global <GLOBAL-ASSOC-LIST-NAME>
```

|                                                                                                                         |                                                                          |
|-------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| <pre><b>association-</b><br/><b>list global</b><br/><b>&lt;GLOBAL-</b><br/><b>ASSOC-LIST-</b><br/><b>NAME&gt;</b></pre> | Associates an existing global association list with this radio interface |
|-------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|

Example

```
rfs4000-880DA7(config-profile-test-if-radio1)#association-list global test

rfs4000-880DA7(config-profile-test-if-radio1)#show context
 interface radio1
 association-list global test
rfs4000-880DA7(config-profile-test-if-radio1)#
```

Related Commands

|                            |                                                                          |
|----------------------------|--------------------------------------------------------------------------|
| <pre>no on page 1114</pre> | Removes the global association list associated with this radio interface |
|----------------------------|--------------------------------------------------------------------------|

beacon

[interface-config-radio-instance](#) on page 1072

Configures radio beacon parameters

A beacon is a packet broadcasted by adopted radios to keep the network synchronized. Included in a beacon is information, such as the WLAN service area, the radio address, the broadcast destination addresses, a time stamp, and indicators about traffic and delivery such as a Delivery Traffic Indication Message (DTIM). Increase the DTIM/beacon settings (lengthening the time) to let nodes sleep longer and preserve battery life. Decrease these settings (shortening the time) to support streaming-multicast audio and video applications that are jitter sensitive.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

Syntax

```
beacon [dtim-period|period]
```

```
beacon dtim-period [<1-50>|bss]
```

```
beacon dtim-period [<1-50>|bss <1-16> <1-50>]
```

beacon period [50|100|200]

Parameters

beacon dtim-period [<1-50>|bss <1-8> <1-50>]

|                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>beacon</b>                                  | Configures radio beacon parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>dtim-period</b>                             | Configures the radio DTIM interval. A DTIM is a message that informs wireless clients about the presence of buffered multicast or broadcast data. These are simple data frames that require no acknowledgement, so nodes sometimes miss them. Increase the DTIM/ beacon settings (lengthening the time) to let nodes sleep longer and preserve their battery life. Decrease these settings (shortening the time) to support streaming multicast audio and video applications that are jitter-sensitive. |
| <b>&lt;1-50&gt;</b>                            | Configures a single value to use on the radio. Specify a value between 1 and 50.                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>bss &lt;1-16&gt;</b><br><b>&lt;1-50&gt;</b> | Configures a separate DTIM for a Basic Service Set (BSS) on this radio interface <ul style="list-style-type: none"><li>• &lt;1-16&gt; - Sets the BSS number from 1 - 16</li><li>• &lt;1-50&gt; - Sets the BSS DTIM from 1 - 50. The default is 2.</li></ul>                                                                                                                                                                                                                                             |

beacon period [50|100|200]

|                            |                                                                                                                                                                                                                                                                                                                            |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>period [50 100 200]</b> | Configures the beacon period (the interval between consecutive radio beacons) <ul style="list-style-type: none"><li>• 50 - Configures 50 K-uSec interval between beacons</li><li>• 100 - Configures 100 K-uSec interval between beacons (default)</li><li>• 200 - Configures 200 K-uSec interval between beacons</li></ul> |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Example

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#beacon dtim-period bss 2 20
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#beacon period 50
```

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#show context
interface radiol
 beacon period 50
 beacon dtim-period bss 1 2
 beacon dtim-period bss 2 20
 beacon dtim-period bss 3 2
 --More--
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#
```

Related Commands

|                        |                                          |
|------------------------|------------------------------------------|
| <b>no</b> on page 1114 | Removes the configured beacon parameters |
|------------------------|------------------------------------------|

bridge

[interface-config-radio-instance](#) on page 1072

Configures the CB (client-bridge) parameters for radios with rf-mode set to bridge. When configured as a client bridge, the radio can authenticate and associate to the WLAN hosted on the infrastructure access point. After successfully associating with the infrastructure WLAN, the CB access point switches frames between its bridge radio and wired/wireless client(s) connected either to its GE port(s) or to the other radio, there by providing the clients access to the infrastructure WLAN resources.

---

This command configures settings that define the authentication-type and encryption-type used by the CB AP to associate and communicate with the infrastructure AP. It also configures other parameters, such as channel-dwell time, wlan ssid, etc.



#### Note

The radio interface configured to form the client-bridge will not be able to service wireless clients as its RF mode is set to bridge and not 2.4 GHz or 5.0 GHz.

---

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7522, AP7532, AP7622, AP7622, AP7632, AP7602, AP7622

Syntax

```
bridge [authentication-type | channel-dwell-time | channel-list | connect-through-bridges | eap | encryption-type | inactivity-timeout | keepalive | max-clients | on-link-loss | on-link-up | roam-criteria | ssid | wpa-wpa2]
```

The following *EAP authentication commands* have been documented in the first five Parameter tables:

```
bridge [authentication-type [eap|none]]
```

```
bridge eap [password|trustpoint|type|username]
```

```
bridge eap type [peap-mschapv2|tls]
```

```
bridge eap password <PASSWORD>
```

```
bridge eap username <USERNAME>
```

```
bridge eap trustpoint [ca|client] <TRUSTPOINT-NAME>
```

```
bridge eap trustpoint on-cert-expiry [continue|discontinue]
```

The following *CB related parameters* have been documented in the last Parameter table:

```
bridge channel-dwell-time <50-2000>
```

```
bridge channel-list [2.4GHz|5GHz] <LIST>
```

```
bridge connect-through-bridges
```

```
bridge encryption-type [ccmp|none|tkip]
```

```
bridge inactivity-timeout <0-864000>
```

```
bridge keepalive [frame-type [null-data|wnmp]]|interval <0-36000>]
```

```
bridge max-clients <1-64>
```

```
bridge on-link-loss shutdown-other-radio <1-1800>
```

```
bridge on-link-up refresh-vlan-interface
```

```
bridge roam-criteria [missed-beacon <1-60>|rssi-threshold <-128--40>]
```

```
bridge ssid <SSID>
```

```
bridge wpa-wpa2 psk <LINE>
```

Parameters

```
bridge [authentication-type [eap|none]]
```

|                                       |                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>bridge</b>                         | Configures client-bridge related parameters on the selected radio<br><br><b>Note:</b> Prior to configuring the client-bridge parameters, set the radio's rf-mode to bridge.                                                                                                                                                                                                                                 |
| <b>authentication-type [eap none]</b> | Configures the authentication framework used between the client-bridge and infrastructure WLAN APs. <ul style="list-style-type: none"><li>• eap – Uses EAP authentication (802.1X).</li><li>• none – Uses no authentication. This is the default setting.</li></ul> <b>Note:</b> If selecting EAP authentication, use the 'bridge > eap > type' command to configure the type of EAP authentication to use. |

```
bridge eap type [peap-mschapv2|tls]
```

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>bridge</b>                       | Configures client-bridge related parameters on the selected radio<br><br><b>Note:</b> Prior to configuring the client-bridge parameters, set the radio's rf-mode to bridge.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>eap type [peap-mschapv2 tls]</b> | If selecting EAP authentication, specify the EAP authentication type to use. The options are: <ul style="list-style-type: none"><li>• PEAP-MSCHAPv2 – Configures EAP authentication type as PEAP-MSCHAPv2. This mode uses a username/password for authentication of the CB AP by the RADIUS server host. This is the default setting.<br/><br/><b>Note:</b> If selecting this option, use the following commands to configure the username and password:<br/><br/>'bridge &gt; eap &gt; username &gt; &lt;USER-NAME&gt;'<br/>'bridge &gt; eap &gt; password &gt; &lt;PASSWORD&gt;'</li><li>• TLS – Configures EAP authentication type as TLS. This mode uses trustpoints (TPs) to authenticate the CB AP and RADIUS server host.<br/><br/><b>Note:</b> If selecting this option, use the 'bridge &gt; eap &gt; trustpoint' command to configure the TPs used for authentication.</li></ul> Ensure that the authentication-type configured on the CB AP is the same as that on the infrastructure WLAN. |

```
bridge eap username <USERNAME>
```

|                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>bridge</b>                                   | Configures client-bridge related parameters on the selected radio<br><br><b>Note:</b> Prior to configuring the client-bridge parameters, set the radio's rf-mode to bridge.                                                                                                                                                                                                                                                                                                               |
| <b>eap username</b><br><b>&lt;UESERNAME&gt;</b> | Configures username used for authentication with the RADIUS server host<br><ul style="list-style-type: none"> <li>• &lt;USERNAME&gt; – Specify the username.</li> </ul> <p><b>Note:</b> PEAP-MSCHAPv2 – For PEAP-MSCHAPv2 authentication. The username specified here should be configured in the RADIUS server policy used on the RADIUS server host.</p> <p>TLS – For TLS authentication, use the username configured in the CN field of the installed PKCS #12 client certificate.</p> |

```
bridge eap password <PASSWORD>
```

|                                                  |                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>bridge</b>                                    | Configures client-bridge related parameters on the selected radio<br><br><b>Note:</b> Prior to configuring the client-bridge parameters, set the radio's rf-mode to bridge.                                                                                                                                                                                               |
| <b>eap password</b><br><b>[&lt;PASSWORD&gt;]</b> | If EAP authentication type is set to PEAP-MSCHAPv2, use this option to configure the password used for authentication. The password specified here should be associated with the username configured in the RADIUS server policy used on the RADIUS server host.<br><ul style="list-style-type: none"> <li>• password &lt;PASSWORD&gt; – Specify the password.</li> </ul> |

```
bridge eap trustpoint [client <TRUSTPOINT-NAME>|ca <TRUSTPOINT-NAME>]
```

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>bridge</b>         | Configures client-bridge related parameters on the selected radio<br><br><b>Note:</b> Prior to configuring the client-bridge parameters, set the radio's rf-mode to bridge.                                                                                                                                                                                                                                                                          |
| <b>eap trustpoint</b> | If EAP authentication type is set to EAP-TLS, use this command to configure TP (trustpoint) details.<br>In EAP-TLS authentication, the CB AP and RADIUS server host authenticate each other using TPs. A TP contains the <i>CA certificate</i> and the <i>CA-signed certificate authenticating</i> the device. To enable TP-based authentication, both the CB AP and the RADIUS server host <b>must</b> use the same CA as the certifying authority. |

**client**  
**<TRUSTPOINT-**  
**NAME>**

Configures the *Client-TP* name (this is the TP installed on the CB AP). When configured, the certificate installed on the CB AP is sent across a TLS tunnel and matched for authentication at the RADIUS server host.

- <TRUSTPOINT-NAME> – Specify the TP name. This configuration is mandatory for enabling TP-based authentication of CB AP.

**Note:** To view TP name, use the **show > crypto > pki > trustpoint** command on the CB AP.

**Note:** On the self of the RADIUS server host, execute the following commands:

**trustpoint > radius-server> <TUSTPOINT-NAME>** - This is the RADIUS server TP name.

**trustpoint > radius-ca > <TUSTPOINT-NAME>** - This is the RADIUS server TP name.

For more information, see [trustpoint \(device-config-mode\)](#) on page 1282.

**ca <TRUSTPOINT-**  
**NAME>**

This configuration is applicable to both the EAP-TLS and PEAP-MSCHAPv2 authentication types. Configure this option only if you want to enable RADIUS server certificate validation at the client end. This configuration is not mandatory for enabling TP-based authentication of CB AP.

- <TRUSTPOINT-NAME> – Specify the TP name (it is the TP installed on the RADIUS server host).

```
bridge eap trustpoint on-cert-expiry [continue|discontinue]]
```

**bridge**

Configures client-bridge related parameters on the selected radio

**Note:** Prior to configuring the client-bridge parameters, set the radio's rf-mode to bridge.

**eap trustpoint**  
**on-cert-expiry**  
**[continue |**  
**discontinue]**

If EAP authentication type is set to EAP-TLS, a CA-signed certificate is used to authenticate the CB AP and RADIUS server host to establish the wireless CB. Use this command to specify whether the wireless CB is to be continued or terminated on expiration of this certificate.

- continue – Enables continuation of the CB even after the certificate (CA/client) has expired. When configured, this option enables automatic CA certificate deployment as and when new CA certificates are available.
- discontinue – Terminates the CB once the certificate (CA/client) has expired.

**Note:** Configure this parameter only if the CB AP and the RADIUS server host are using a crypto CMP policy for automatic certificate renewal. For more information, see [CRYPTO-CMP-POLICY](#) on page 1831.

```
bridge [channel-dwell-time <50-2000>|channel-list [2.4GHz|5GHz] <LIST>|
connect-through-bridges|encryption-type [ccmp|none|tkip]|inactivity-timeout <0-864000>|
keepalive [frame-type [null-data|wnmp]|interval <0-36000>]|max-clients <1-64>|
on-link-loss shutdown-other-radio <1-1800>|on-link-up refresh-vlan-interface|
roam-criteria [missed-beacons <1-60>|ssid <SSID>|wpa-wpa2 psk [0|2|<LINE>]]
```



|                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>bridge</b>                                                               | <p>Configures client-bridge related parameters on the selected radio</p> <p><b>Note:</b> Prior to configuring the client-bridge parameters, set the radio's rf-mode to bridge.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>channel-dwell-time &lt;50-2000&gt;</b>                                   | <p>Configures the channel-dwell time in milliseconds. This is the time the client-bridge radio dwells on each channel (configured in the channel-list) when scanning for an infrastructure WLAN.</p> <ul style="list-style-type: none"> <li>• &lt;50-2000&gt; - Specify a value from 50 -2000 milliseconds. The default is 150 milliseconds.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>channel-list [2.4GHz   5GHz] &lt;LIST&gt;</b>                            | <p>Configures the list of channels the radio scans when scanning for an infrastructure WLAN access point to associate</p> <ul style="list-style-type: none"> <li>• 2.4GHz &lt;LIST&gt; - Configures a list of channels for scanning across all the channels in the 2.4GHz radio band</li> <li>• 5GHz &lt;LIST&gt; - Configures a list of channels for scanning across all the channels in the 5.0 GHz radio band</li> </ul> <p>The following parameter is common to both of the 2.4 GHZ and 5.0 GHz bands:</p> <ul style="list-style-type: none"> <li>• &lt;LIST&gt; - Provide the list of channels separated by commas.</li> </ul>                                                                                                                                               |
| <b>connect-through-bridges</b>                                              | <p>Enables the client-bridge access point radio to connect to an infrastructure WLAN, which already has other client-bridge radios associated with it. The client-bridge access points, in this scenario, are said to be daisy chained together.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>encryption-type [ccmp   none   tkip]</b>                                 | <p>Configures the encryption mode. The encryption mode specified here should be the same as that configured on the infrastructure WLAN. The options are:</p> <ul style="list-style-type: none"> <li>• ccmp - Uses WPA/WPA2 CCMP encryption</li> <li>• none - Uses no encryption method. This is the default setting.</li> <li>• tkip - Uses WPA/WPA2 TKIP encryption</li> </ul> <p>If using CCMP or TKIP, use the 'wpa2-wpa2' keyword to configure the pre-shared key (PSK).</p>                                                                                                                                                                                                                                                                                                  |
| <b>inactivity-timeout &lt;0-864000&gt;</b>                                  | <p>Configures the inactivity timeout for each bridge MAC address. This is the time for which the client-bridge access point waits before deleting a MAC address from which a frame has not been received for more than the time specified here. For example, if the inactivity time is set at 120 seconds, and if no frames are received from a MAC address for 120 seconds, it is deleted. The default value is 600 seconds.</p> <ul style="list-style-type: none"> <li>• &lt;0-864000&gt; - Specify a value from 0 - 864000 seconds. The default is 600 seconds.</li> </ul>                                                                                                                                                                                                     |
| <b>keepalive [frame-type [null-data   wnmp]   interval &lt;0-36000&gt;]</b> | <p>Configures the keep-alive frame type and interval</p> <ul style="list-style-type: none"> <li>• frame-type - Configures the keepalive frame type exchanged between the client-bridge access point and the infrastructure access point/controller. The options are: <ul style="list-style-type: none"> <li>• null-data - Transmits 802.11 NULL data frames. This is the default setting.</li> <li>• wnmp - Transmits Wireless Network Management Protocol (WNMP) multicast packet</li> </ul> </li> <li>• interval &lt;0-36000&gt; - Configures the interval, in seconds, between successive keep-alive frame transmission. <ul style="list-style-type: none"> <li>• &lt;0-36000&gt; - Specify a value from 0 - 36000 seconds. The default is 300 seconds.</li> </ul> </li> </ul> |
| <b>max-clients &lt;1-64&gt;</b>                                             | <p>Configures the maximum number of clients that the client-bridge AP can support</p> <ul style="list-style-type: none"> <li>• &lt;1-14&gt; - Specify a value from 1 - 64. The default is 64.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

|                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>on-link-loss shutdown-other-radio &lt;1-1800&gt;</b>                              | <p>Configures the radio-link behaviour when the link between the client-bridge and infrastructure access points is lost.</p> <ul style="list-style-type: none"> <li>shutdown-other-radio – Enables shutting down of the non-client bridge radio (this is the radio to which wireless-clients associate) when the link between the client-bridge and infrastructure access points is lost. When enabled, clients associated with the non-client bridge radio are pushed to search for and associate with other access points having backhaul connectivity. This option is disabled by default.</li> <li>&lt;1-1800&gt; – If enabling this option, use this parameter to configure the time, in seconds, for which the non-client bridge radio is shut down. Specify a value from 1 - 1800 seconds.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>on-link-up refresh-vlan-interface</b>                                             | <p>Configures the radio-link behaviour when the link between the client-bridge and infrastructure access points comes up.</p> <ul style="list-style-type: none"> <li>refresh-vlan-interface – Enables the SVI to refresh on re-establishing client bridge link to infrastructure Access Point. And, if using a DHCP assigned IP address, causes a DHCP renew. This option is enabled by default.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>roam-criteria [missed-beacons &lt;1-60&gt;   rssi-threshold &lt;-128--40&gt;]</b> | <p>Configures the following roaming criteria parameters</p> <ul style="list-style-type: none"> <li>missed-beacons &lt;1-60&gt; – Configures the missed beacon interval from 0 - 60 seconds. This is the time for which the CB AP waits for, after missing a beacon from the associated infrastructure AP, before roaming to another infrastructure AP. For example, if the missed-beacon time is set to 30 seconds, and if more than 30 seconds have passed since the last received beacon, the CB AP resumes scanning for another infrastructure AP. The default value is 20 seconds. <ul style="list-style-type: none"> <li>&lt;1-60&gt; – Specify a value from 1 - 60 seconds. The default is 20 seconds.</li> </ul> </li> <li>rssi-threshold &lt;-128--40&gt; – Configures the minimum signal strength, received from target AP, for the bridge connection to be maintained before roaming <ul style="list-style-type: none"> <li>&lt;-128--40&gt; – Specify a value from -128 - -40 dBm. If the RSSI value of infrastructure access point radio signals falls below the specified value, the CB AP resumes scanning for another infrastructure access point. The default is -75 dBm.</li> </ul> </li> </ul> |
| <b>ssid &lt;SSID&gt;</b>                                                             | <p>Configures the infrastructure WLAN SSID the client bridge connects to</p> <ul style="list-style-type: none"> <li>&lt;SSID&gt; – Specify the SSID.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>wpa-wpa2 psk &lt;LINE&gt;</b>                                                     | <p>Configures the encryption PSK to use with the infrastructure WLAN</p> <ul style="list-style-type: none"> <li>&lt;LINE&gt; – Enter the key</li> </ul> <p><b>Note:</b> Pre-shared keys are valid only when the authentication-type is set to none and the encryption-type is set to tkip or ccmp.<br/>The PSK should be 8 - 32 characters in length.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

#### Usage Guidelines EAP Authentication

Use the following commands to view client-bridge configuration:

1 show > wireless > bridge > config

Shows the current client bridge configuration.

2 show > wireless > bridge > candidate-ap

Shows the available infrastructure WLAN candidates that are found during the last scan.

3 show > wireless > bridge > host

Shows the wired/wireless clients that are being bridged.

- 4 show > wireless > bridge > statistics > rf

Shows the client bridge RF statistics.

- 5 show > wireless > bridge > statistics > traffic

Shows the client bridge traffic statistics.

- 6 show > wireless > bridge > certificate > status

Shows the client bridge authentication certificate status.

Use the following command on the CB AP and the RADIUS server host to view installed TP details:

- 1 show > crypto > pki > trustpoints

### Example - CB with authentication 'none' and encryption 'ccmp'

The following example shows the basic parameters that need to be configured on the Infrastructure and the CB APs in order to enable the CB AP to associate with the Infrastructure WLAN. Note, in this example, the authentication mode is set to 'none' and the encryption-type is set to 'ccmp'. The authentication and encryption modes used will vary as per requirement.

- 1 Configure the Infrastructure WLAN:

```
InfrastrNOC(config)#show running-config wlan cb-psk
wlan cb-psk
ssid cb-psk
bridging-mode local
encryption-type ccmp
authentication-type none
wpa-wpa2 psk 0 extreme@123
```

```
InfrastrNOC(config)#
```

- 2 Associate the 'cb-psk' WLAN to the Infrastructure AP.

```
InfrastrAP(config-device-B4-C7-99-5F-50-78-if-radio2)#wlan cb-psk
```

- 3 Confirm the Infrastructure AP's radio interface status.

```
InfrastrAP(config)#show wireless radio

RADIO RADIO-MAC RF-MODE STATE CHANNEL POWER
#CLIENT

InfrastrAP:R1 B4-C7-99-5E-51-40 2.4GHz-wlan Off N/A (smt) 0 (smt) 0
InfrastrAP:R2 B4-C7-99-5E-1A-40 5GHz-Wlan On 165 (165) 17 (smt) 2

Total number of radios displayed: 2
InfrastrAP(config)#
```

- 4 Configure following radio parameters on the CB AP:

```
ClientBridgeAP(config-device-84-24-8D-85-B2-74-if-radio2)#rf-mode bridge
```

```
ClientBridgeAP(config-device-84-24-8D-85-B2-74-if-radio2)#bridge ssid cb-psk
```

```
ClientBridgeAP(config-device-84-24-8D-85-B2-74-if-radio2)#bridge encryption-type ccmp
```

```
ClientBridgeAP(config-device-84-24-8D-85-B2-74-if-radio2)#bridge authentication-type none
```

```
ClientBridgeAP(config-device-84-24-8D-85-B2-74-if-radio2)#bridge wpa-wpa2 psk
extreme@123
```

```
ClientBridgeAP(config-device-84-24-8D-85-B2-74-if-radio2)#show context
interface radio2
 rf-mode bridge
 bridge ssid cb-psk
 bridge encryption-type ccmp
 bridge wpa-wpa2 psk 0 extreme@123
ClientBridgeAP(config-device-84-24-8D-85-B2-74-if-radio2)#
```

Note, bridge SSID, encryption-type, and authentication mode are the same as that of the Infrastructure WLAN.

- 5 Confirm the CB AP's radio interface status.

```
ClientBridgeAP#show wireless radio

RADIO RADIO-MAC RF-MODE STATE CHANNEL POWER
#CLIENT

ClientBridgeAP:R1 84-24-8D-AC-2D-B0 2.4GHz-wlan Off N/A (smt) 0
(smt) 0
ClientBridgeAP:R2 84-24-8D-AC-CC-10 bridge On 165 (smt) 20
(smt) 0

Total number of radios displayed: 2
=====
ClientBridgeAP(config-device-84-24-8D-85-B2-74)#
```

- 6 View the candidate-ap (connected Infrastructure AP's) details on the CB AP.

```
ClientBridgeAP(config-device-84-24-8D-85-B2-74)#show wireless bridge candidate-ap
84-24-8D-AC-CC-10 Client Bridge Candidate APs:
 AP-MAC BAND CHANNEL SIGNAL(dbm) STATUS
 B4-C7-99-5E-1A-40 5 GHz 165 -21 selected
Total number of candidates displayed: 1
Total number of client bridges displayed: 1
=====
ClientBridgeAP(config-device-84-24-8D-85-B2-74)#
```

- 7 View the bridge host details on the CB AP.

```
ClientBridgeAP(config-device-84-24-8D-85-B2-74)#show wireless bridge hosts

HOST MAC BRIDGE MAC IP BRIDGING STATUS ACTIVITY
 (sec ago)

84-24-8D-85-B2-74 84-24-8D-AC-CC-10 10.1.0.249 UP 00:00:07

Total number of hosts displayed: 1
ClientBridgeAP(config-device-84-24-8D-85-B2-74)#
```

### Example - CB with encryption 'CCMP' and authentication 'EAP-TLS' using Trustpoint Client.

- 1 On the Infrastructure AP,
  - a Configure WLAN as shown below.

```
InfrastrAP7532(config)#show running-config wlan cb-tp
wlan cb-tp
 ssid cb-tp
 bridging-mode local
 encryption-type ccmp
```

```
authentication-type eap
InfraStrAP7532(config)#
```

- b Associate WLAN to the infrastructure AP radio.

```
InfraStrAP(config-device-B4-C7-99-5F-50-78-if-radio2)#show context
interface radio2
 wlan cb-tp bss 1 primary
InfraStrAP(config-device-B4-C7-99-5F-50-78-if-radio2)#
```

- c Confirm infrastructure AP's radio interface status.

```
InfraStrAP(config)#show wireless radio
```

```

RADIO RADIO-MAC RF-MODE STATE CHANNEL
POWER #CLIENT

InfraStrAP:R1 B4-C7-99-5E-51-40 2.4GHz-wlan Off N/A (smt) 0 (smt)
0
InfraStrAP:R2 B4-C7-99-5E-1A-40 5GHz-Wlan On 165 (165) 17 (smt)
2

```

```
Total number of radios displayed: 2
InfraStrAP(config)#
```

- 2 On the RADIUS server host,

- a Configure the RADIUS user policy as shown below:

```
RADServer(config-radius-user-pool-cb-tp)#show context
radius-user-pool-policy cb-tp
 user admin password 0 extreme@123
RADServer(config-radius-user-pool-cb-tp)#
```



#### Note

In case of EAP-TLS authentication, the username configured here should be the "common name" on the client certificate.

- b Use this RADIUS user policy in the RADIUS server policy.

```
RADServer(config-radius-server-policy-cb-tp)#show context
radius-server-policy cb-tp
 use radius-user-pool-policy cb-tp
RADServer(config-radius-server-policy-cb-tp)#
```

- c On the self of the RADIUS server host,

- Apply the RADIUS server policy.  

```
RADServer(config-device-74-67-F7-07-02-35)#use radius-server-policy cb-tp
```
- Configure the trustpoint to be used to authenticate the RADIUS server host and RADIUS server CA.  

```
RADServer(config-device-74-67-F7-07-02-35)#trustpoint radius-server serverTP
RADServer(config-device-74-67-F7-07-02-35)#trustpoint radius-ca serverTP
```



#### Note

Ensure that the trustpoint is existing and installed on the RADIUS server. Also ensure that the RADIUS server host and CB AP are using the same CA for certification.

- 3 On the CB AP,

- a Configure the mandatory parameters as shown below:

```
clientbriAP(config-device-84-24-8D-DF-9A-4C-if-radio2)#show context
interface radio2
 rf-mode bridge
```

```

channel smart
power smart
data-rates default
no preamble-short
bridge ssid cb-tp
bridge encryption-type ccmp
bridge authentication-type eap
bridge eap username admin
bridge eap trustpoint client clientTP
bridge eap type tls
clientbriAP(config-device-84-24-8D-DF-9A-4C-if-radio2)#

```



#### Note

In case of EAP-TLS authentication, the username configured here should be the “common name” on the client certificate.



#### Note

Ensure that the CB AP and RADIUS server host are using the same CA for certification.

- b If you want to enable RADIUS server certificate validation at the client end, execute the following command:

```
clientbriAP(config-device-84-24-8D-DF-9A-4C-if-radio2)#trustpoint radius-ca clientTP
```



#### Note

This is an optional parameter that provides additional security and is applicable for EAP-TLS and PEAP-MSCHAPv2 authentication modes.

### Related Commands

|                              |                                               |
|------------------------------|-----------------------------------------------|
| <code>no</code> on page 1114 | Removes or resets this client-bridge settings |
|------------------------------|-----------------------------------------------|

### channel

[interface-config-radio-instance](#) on page 1072

Configures a radio’s channel of operation

Only a trained installation professional should define the radio channel. Select Smart for the radio to scan non-overlapping channels listening for beacons from other access points. After the channels are scanned, the radio selects the channel with the fewest access points. In case of multiple access points on the same channel, it selects the channel with the lowest average power level.



#### Note

Channels with a “w” appended to them are unique to the 40 MHz band. Channels with a “ww” appended to them are 802.11ac specific, and appear only when using an and are unique to the 80 MHz band.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

Syntax

```
channel [smart | acs | random | 1 | 2 | 3 | 4 | -----]
```

## Parameters

channel [smart|acs|random|1|2|3|4|-----]

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>channel</b>                          | Configures a radio's channel of operation                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>[smart acs random 1 2 3 4 -----]</b> | Configures a radio's channel of operation. The options are: <ul style="list-style-type: none"><li>• smart - Uses Smart RF to assign a channel (uses uniform spectrum spreading if Smart RF is not enabled). This is the default setting.</li><li>• acs - Uses automatic channel selection (ACS) to assign a channel</li><li>• random - Randomly assigns a channel</li><li>• 1 - Channel 1 in 20 MHz mode</li><li>• 2 - Channel 2 in 20 MHz mode</li></ul> |

## Example

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radio1)#channel 1

nx9500-6C8809(config-profile-7lxxTestProfile-if-radio1)#show context
interface radio1
 channel 1
 beacon period 50
 beacon dtim-period bss 1 5
 beacon dtim-period bss 2 2

 beacon dtim-period bss 14 5
 beacon dtim-period bss 15 5
 beacon dtim-period bss 16 5
 antenna-gain 12.0
 aggregation ampdu tx-only
 aeroscout forward
 antenna-mode 2x2
 antenna-diversity
--More--
nx9500-6C8809(config-profile-7lxxTestProfile-if-radio1)#
```

## Related Commands

|                        |                                       |
|------------------------|---------------------------------------|
| <b>no</b> on page 1114 | Resets a radio's channel of operation |
|------------------------|---------------------------------------|

## data-rates

[interface-config-radio-instance](#) on page 1072

Configures the 802.11 data rates on this radio

This command sets the rate options depending on the 802.11 protocol and the radio band selected. If 2.4 GHz is selected as the radio band, select separate 802.11b, 802.11g and 802.11n rates and define how they are used in combination. If 5.0 GHz is selected as the radio band, select separate 802.11a and 802.11n rates then define how they are used together.

If dedicating the radio to either 2.4 or 5.0 GHz support, use the custom keyword to set a 802.11n modulation and coding scheme (MCS) in respect to the radio's channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Clients can associate as long as they support basic MCS (as well as non-11n basic rates).

Data rates are fixed and not user configurable for radios functioning as sensors.



#### Note

Use the `rf-mode` command to configure a radio's mode of operation.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

Syntax

```
data-rates [b-only|g-only|a-only|bg|bgn|gn|an|default|custom|mcs]
```

```
data-rates [b-only|g-only|a-only|bg|bgn|gn|an|default]
```

```
data-rates custom [1|2|5.5|6|9|11|12|18|24|36|48|54|mcs-1s|mcs-2s|mcs-3s|
basic-1|basic-2|basic-5.5|basic-6|basic-9|basic-11|basic-12|basic-18|
basic-24|basic-36|basic-48|basic-54|basic-mcs-1s]
```

```
data-rates mcs qam-only
```

Parameters

```
data-rates [b-only|g-only|a-only|bg|bgn|gn|an|default]
```

|                   |                                                                                                               |
|-------------------|---------------------------------------------------------------------------------------------------------------|
| <b>data-rates</b> | Configures the 802.11 data rates on this radio                                                                |
| <b>b-only</b>     | Supports operation in the 802.11b mode only (applicable for 2.4 and 4.9 GHz bands)                            |
| <b>g-only</b>     | Uses rates that support operation in the 802.11g mode only (applicable for 2.4 and 4.9 GHz bands)             |
| <b>a-only</b>     | Uses rates that support operation in the 802.11a mode only (applicable for 5.0 GHz band only)                 |
| <b>bg</b>         | Uses rates that support 802.11b and 802.11g wireless clients (applicable for 2.4 and 4.9 GHz bands)           |
| <b>bgn</b>        | Uses rates that support 802.11b, 802.11g, and 802.11n wireless clients (applicable for 2.4 and 4.9 GHz bands) |
| <b>gn</b>         | Uses rates that support 802.11g and 802.11n wireless clients (applicable for 2.4 and 4.9 GHz bands)           |
| <b>an</b>         | Uses rates that support 802.11a and 802.11n wireless clients (applicable for 5.0 GHz band only)               |
| <b>default</b>    | Enables the default data rates according to the radio's band of operation                                     |

```
data-rates custom [1|2|5.5|6|9|11|12|18|24|36|48|54|mcs-1s|mcs-2s|mcs-3s|basic-1|basic-2|
basic-5.5|basic-6|basic-9|basic-11|basic-12|basic-18|basic-24|basic-36|basic-48|basic-54|
basic-mcs-1s]
```



|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>data-rates</b> | Configures the 802.11 data rates on this radio                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>custom</b>     | <p>Configures a list of data rates by specifying each rate individually. Use 'basic-' prefix before a rate to indicate it's used as a basic rate (For example, 'data-rates custom basic-1 basic-2 5.5 11')</p> <ul style="list-style-type: none"> <li>• 1 - 1-Mbps</li> <li>• 2 - 2-Mbps</li> <li>• 5.5 - 5.5-Mbps</li> <li>• 6 - 6-Mbps</li> <li>• 9 - 9-Mbps</li> <li>• 11 - 11-Mbps</li> <li>• 12 - 12-Mbps</li> <li>• 18 - 18-Mbps</li> <li>• 24 - 24-Mbps</li> <li>• 36 - 36-Mbps</li> <li>• 48 - 48-Mbps</li> <li>• 54 - 54-Mbps</li> <li>• mcs-1s - Applicable to 1-spatial stream data rates</li> <li>• mcs-2s - Applicable to 2-spatial stream data rates</li> <li>• mcs-3s - Applicable to 3-spatial stream data rates</li> <li>• basic-1 - Basic 1-Mbps</li> <li>• basic-2 - Basic 2-Mbps</li> <li>• basic-5.5 - Basic 5.5-Mbps</li> <li>• basic-6 - Basic 6-Mbps</li> <li>• basic-9 - Basic 9-Mbps</li> <li>• basic-11 - Basic 11-Mbps</li> <li>• basic-12 - Basic 12-Mbps</li> <li>• basic-18 - Basic 18-Mbps</li> <li>• basic-24 - Basic 24-Mbps</li> <li>• basic-36 - Basic 36-Mbps</li> </ul> |
|                   | <ul style="list-style-type: none"> <li>• basic-48 - Basic 48-Mbps</li> <li>• basic-54 - Basic 54-Mbps</li> <li>• basic-mcs-1s - Modulation and Coding Scheme data rates for 1 Spatial Stream</li> </ul> <p><b>Note:</b> Refer to the Usage Guidelines <a href="#">Usage Guidelines (Supported data rates)</a> on page 1101 section for 802.11an and 802.11ac MCS detailed data rates for both with and without short guard intervals (SGI).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

`data-rates mcs qam-only`

|                     |                                                 |
|---------------------|-------------------------------------------------|
| <b>data-rates</b>   | Configures the 802.11 data rates on this radio  |
| <b>mcs qam-only</b> | Configures supports for MCS QAM data rates only |

Usage Guidelines (Supported data rates)

The following table defines the 802.11n MCS for MCS 1 streams, both with and without SGI:



| <b>MCS-1Stream Index</b> | <b>Number of Streams</b> | <b>20 MHz No SGI</b> | <b>20 MHz With SGI</b> | <b>40 MHz No SGI</b> | <b>20 MHz With SGI</b> |
|--------------------------|--------------------------|----------------------|------------------------|----------------------|------------------------|
| 0                        | 1                        | 6.5                  | 7.2                    | 13.5                 | 15                     |
| 1                        | 1                        | 13                   | 14.4                   | 27                   | 30                     |
| 2                        | 1                        | 19.5                 | 21.7                   | 40.5                 | 45                     |
| 3                        | 1                        | 26                   | 28.9                   | 54                   | 60                     |
| 4                        | 1                        | 39                   | 43.4                   | 81                   | 90                     |
| 5                        | 1                        | 52                   | 57.8                   | 108                  | 120                    |
| 6                        | 1                        | 58.5                 | 65                     | 121.5                | 135                    |
| 7                        | 1                        | 65                   | 72.2                   | 135                  | 150                    |

The following table defines the 802.11n MCS for MCS 2 streams, both with and without SGI:

| <b>MCS-2Stream Index</b> | <b>Number of Streams</b> | <b>20 MHz No SGI</b> | <b>20 MHz With SGI</b> | <b>40 MHz No SGI</b> | <b>20 MHz With SGI</b> |
|--------------------------|--------------------------|----------------------|------------------------|----------------------|------------------------|
| 0                        | 2                        | 13                   | 14.4                   | 27                   | 30                     |
| 1                        | 2                        | 26                   | 28.9                   | 54                   | 60                     |
| 2                        | 2                        | 39                   | 43.4                   | 81                   | 90                     |
| 3                        | 2                        | 52                   | 57.8                   | 108                  | 120                    |
| 4                        | 2                        | 78                   | 86.7                   | 162                  | 180                    |
| 5                        | 2                        | 104                  | 115.6                  | 216                  | 240                    |
| 6                        | 2                        | 117                  | 130                    | 243                  | 270                    |
| 7                        | 2                        | 130                  | 144.4                  | 270                  | 300                    |

The following table defines the 802.11n MCS for MCS 3 streams, both with and without SGI:

| <b>MCS-3Stream Index</b> | <b>Number of Streams</b> | <b>20 MHz No SGI</b> | <b>20 MHz With SGI</b> | <b>40 MHz No SGI</b> | <b>20 MHz With SGI</b> |
|--------------------------|--------------------------|----------------------|------------------------|----------------------|------------------------|
| 0                        | 3                        | 19.5                 | 21.7                   | 40.5                 | 45                     |
| 1                        | 3                        | 39                   | 43.3                   | 81                   | 90                     |
| 2                        | 3                        | 58.5                 | 65                     | 121.5                | 135                    |
| 3                        | 3                        | 78                   | 86.7                   | 162                  | 180                    |
| 4                        | 3                        | 117                  | 130.7                  | 243                  | 270                    |
| 5                        | 3                        | 156                  | 173.3                  | 324                  | 360                    |
| 6                        | 3                        | 175.5                | 195                    | 364.5                | 405                    |
| 7                        | 3                        | 195                  | 216.7                  | 405                  | 450                    |

The following table defines the 802.11ac MCS rates (theoretical throughput for single spatial streams) both with and without SGI:

| MCS Index | 20 MHz No SGI | 20 MHz With SGI | 40 MHz No SGI | 40 MHz With SGI | 80 MHz No SGI | 80 MHz No SGI |
|-----------|---------------|-----------------|---------------|-----------------|---------------|---------------|
| 0         | 6.5           | 7.2             | 13.5          | 15              | 29.3          | 32.5          |
| 1         | 13            | 14.4            | 27            | 30              | 58.5          | 65            |
| 2         | 19.5          | 21.7            | 40.5          | 45              | 87.8          | 97.5          |
| 3         | 26            | 28.9            | 54            | 60              | 117           | 130           |
| 4         | 39            | 43.3            | 81            | 90              | 175.5         | 195           |
| 5         | 52            | 57.8            | 108           | 120             | 234           | 260           |
| 6         | 58.5          | 65              | 121.5         | 135             | 263.3         | 292.5         |
| 7         | 65            | 72.2            | 135           | 150             | 292.5         | 325           |
| 8         | 78            | 86.7            | 162           | 180             | 351           | 390           |
| 9         | N/A           | N/A             | 180           | 200             | 390           | 433.3         |

#### Example

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radio1)#data-rates b-only
```

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radio1)#show context
```

```
interface radio1
 channel 1
 data-rates b-only
 beacon period 50
 beacon dtim-period bss 1 5
 beacon dtim-period bss 2 2
 beacon dtim-period bss 3 5

 beacon dtim-period bss 13 5
 beacon dtim-period bss 14 5
 beacon dtim-period bss 15 5
 beacon dtim-period bss 16 5
 antenna-gain 12.0
 aggregation ampdu tx-only
 aeroscout forward
 --More--
```

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radio1)#
```

#### Related Commands

|                                      |                                             |
|--------------------------------------|---------------------------------------------|
| <a href="#">no</a> on page 1114      | Resets the 802.11 data rates on a radio     |
| <a href="#">rf-mode</a> on page 1127 | Configures the radio's RF mode of operation |

description

[interface-config-radio-instance](#) on page 1072

Configures the selected radio's description that helps differentiate it from other radios with similar configurations

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

#### Syntax

**description** <WORD>

#### Parameters

**description** <WORD>

|                                           |                                                                                           |
|-------------------------------------------|-------------------------------------------------------------------------------------------|
| <b>description</b><br><b>&lt;WORD&gt;</b> | Provide a description for the selected radio (should not exceed 64 characters in length). |
|-------------------------------------------|-------------------------------------------------------------------------------------------|

#### Example

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#description "Primary radio to use"
```

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#show context
interface radiol
 description "Primary radio to use"
 channel 1
 data-rates b-only
 beacon period 50
 beacon dtim-period bss 1 5
 beacon dtim-period bss 2 2
 beacon dtim-period bss 3 5
 beacon dtim-period bss 4 5
 beacon dtim-period bss 5 5
 beacon dtim-period bss 6 5
 beacon dtim-period bss 7 5
 beacon dtim-period bss 8 5
 beacon dtim-period bss 9 5
 beacon dtim-period bss 10 5
 beacon dtim-period bss 11 5
 beacon dtim-period bss 12 5
 beacon dtim-period bss 13 5
 beacon dtim-period bss 14 5
 beacon dtim-period bss 15 5
 beacon dtim-period bss 16 5
 antenna-gain 12.0
 aggregation ampdu tx-only
--More--
nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#
```

#### Related Commands

|                                 |                               |
|---------------------------------|-------------------------------|
| <a href="#">no</a> on page 1114 | Removes a radio's description |
|---------------------------------|-------------------------------|

#### dfs-rehome

[interface-config-radio-instance](#) on page 1072

Reverts to configured home channel once the Dynamic Frequency Selection (DFS) evacuation period expires



#### Note

This option is applicable only if the radio's RF mode is set to '5GHz-wlan'.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

#### Syntax

```
dfs-rehome {holdtime <30-3600>}
```

#### Parameters

```
dfs-rehome {holdtime <30-3600>}
```

|                                                                  |                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>dfs-rehome</b><br><b>{holdtime</b><br><b>&lt;30-3600&gt;}</b> | <p>Enables the radio to revert to the configured home channel once the DFS evacuation period expires</p> <ul style="list-style-type: none"> <li>• holdtime - Optional. Specifies the duration, in minutes, to stay in the new channel</li> <li>• &lt;30-3600&gt; - Specify the holdtime from 30 - 3600 minutes. The default is 90 minutes.</li> </ul> |
|------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Example

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#dfs-rehome holdtime 500
```

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#show context
interface radiol
 dfs-rehome holdtime 500
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#
```

#### Related Commands

|                                 |                                                              |
|---------------------------------|--------------------------------------------------------------|
| <a href="#">no</a> on page 1114 | Stays on DFS elected channel after evacuation period expires |
|---------------------------------|--------------------------------------------------------------|

### dynamic-chain-selection

[interface-config-radio-instance](#) on page 1072

Enables automatic antenna mode selection. When enabled, the radio can dynamically change the number of transmit chains used (uses a single chain/antenna for frames at non-11n transmit rates). This option is enabled by default.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

#### Syntax

```
dynamic-chain-selection
```

#### Parameters

None

#### Example

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#dynamic-chain-selection
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#
```

#### Related Commands

|                                 |                                                           |
|---------------------------------|-----------------------------------------------------------|
| <a href="#">no</a> on page 1114 | Uses the configured transmit antenna mode for all clients |
|---------------------------------|-----------------------------------------------------------|

### ekahau

[interface-config-radio-instance](#) on page 1072

Enables Ekahau multicast packet forwarding. When enabled, Ekahau small, battery powered Wi-Fi tags are attached to tracked assets or assets carried by people. Ekahau processes locations, rules, messages, and environmental data and turns the information into locating maps, alerts and reports.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

Syntax

```
ekahau [forward ip <IP> port <0-65535>|mac <MAC>]
```

Parameters

```
ekahau [forward ip <IP> port <0-65535>|mac <MAC>]
```

|                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ekahau</b>                                     | Enables Ekahau multicast packet forwarding on this radio                                                                                                                                                                                                                                                                                                                                                                        |
| <b>forward ip &lt;IP&gt; port &lt;0-65535&gt;</b> | <p>Enables multicast packet forwarding to the Ekahau engine</p> <ul style="list-style-type: none"> <li>• ip &lt;IP&gt; - Configures the IP address of the Ekahau engine in the A.B.C.D format</li> <li>• port &lt;0-65535&gt; - Specifies the TaZman Sniffer Protocol (TZSP) port on Ekahau engine from 0 - 65535</li> </ul> <p>TZSP is an encapsulation protocol, which is generally used to wrap 802.11 wireless packets.</p> |
| <b>mac &lt;MAC&gt;</b>                            | <p>Configures the multicast MAC address to forward the Ekahau multicast packets</p> <ul style="list-style-type: none"> <li>• &lt;MAC&gt; - Specify the MAC address in the AA-BB-CC-DD-EE-FF format.</li> </ul>                                                                                                                                                                                                                  |

Example

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#ekahau forward ip 172.16.10.1 port 3
```

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#show context
```

```
interface radiol
 description "Primary radio to use"
 channel 1
 data-rates b-only
 beacon period 50
 beacon dtim-period bss 1 5
 beacon dtim-period bss 2 2
 beacon dtim-period bss 3 5
 beacon dtim-period bss 4 5
 beacon dtim-period bss 5 5
 beacon dtim-period bss 6 5
 beacon dtim-period bss 7 5

 beacon dtim-period bss 16 5
 antenna-gain 12.0
 aggregation ampdu tx-only
 aeroscout forward
 ekahau forward ip 172.16.10.1 port 3
 antenna-mode 2x2
```

```
--More--
```

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#
```

Related Commands

|                                 |                                           |
|---------------------------------|-------------------------------------------|
| <a href="#">no</a> on page 1114 | Uses default Ekahau multicast MAC address |
|---------------------------------|-------------------------------------------|

extended-range

[interface-config-radio-instance](#) on page 1072

Enables the extended range capability for AP7161 model access point. When enabled, these access points can exchange signals with their clients at greater distances without being timed out. This option is disabled by default.

Supported in the following platforms:

- Access Point — AP7161

Syntax

`extended-range <1-25>`

Parameters

`extended-range <1-25>`

|                                              |                                                                                                                                         |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <b>extended-range</b><br><b>&lt;1-25&gt;</b> | Configures extended range on this radio interface from 1 - 25 kilometers. The default is 2 km on 2.4 GHz band and 7 km on 5.0 GHz band. |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|

Example

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#extended-range 15
```

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#show context
```

```
interface radiol
 description "Primary radio to use"
 channel 1
 data-rates b-only
 beacon period 50
 beacon dtim-period bss 1 5
 beacon dtim-period bss 2 2
 beacon dtim-period bss 3 5
 beacon dtim-period bss 4 5
 beacon dtim-period bss 5 5
 beacon dtim-period bss 6 5
 beacon dtim-period bss 7 5
 beacon dtim-period bss 8 5
 beacon dtim-period bss 9 5
 beacon dtim-period bss 10 5
 beacon dtim-period bss 11 5
 beacon dtim-period bss 12 5
 beacon dtim-period bss 13 5
 beacon dtim-period bss 14 5
 beacon dtim-period bss 15 5
 beacon dtim-period bss 16 5
 antenna-gain 12.0
 aggregation ampdu tx-only
 aeroscout forward
 ekahau forward ip 172.16.10.1 port 3
 antenna-mode 2x2
 antenna-diversity
 airtime-fairness prefer-ht weight 6
 extended-range 15
```

--More--

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#
```

Related Commands

|                                 |                                                                              |
|---------------------------------|------------------------------------------------------------------------------|
| <a href="#">no</a> on page 1114 | Resets the extended range to default (7 km for 2.4 GHz and 5 km for 5.0 GHz) |
|---------------------------------|------------------------------------------------------------------------------|

[fallback-channel](#)

[interface-config-radio-instance](#) on page 1072

Configures the channel to which the radio switches in case of radar detection on the current channel

Supported in the following platforms:

- Access Points – AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

Syntax

```
fallback-channel [100|100w|100ww|104|104w|104ww|108|108w.....]
```

Parameters

```
fallback-channel [100|100w|100ww|104|104w|104ww|108|108w.....]
```

|                                                                       |                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>fallback-channel [100 100w 100ww 104 104w 104ww 108 108w.....]</b> | Configures the fallback channel. This is the channel the radio switches to in case a radar is detected on the radio's current operating channel. <ul style="list-style-type: none"><li>• [100 100w 100ww ...] - Select the fall back channel from the available options.</li></ul> |
|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Example

```
nx9500-6C8809(config-profile-testAP81XX-if-radio2)#fallback-channel 104
```

NOTE: Functionality is supported only in the US regulatory domain and only a non-dfs channel can be configured as a fallback channel

```
nx9500-6C8809(config-profile-testAP81XX-if-radio2)#show context
interface radio2
 fallback-channel 104
nx9500-6C8809(config-profile-testAP81XX-if-radio2)#
```

Related Commands

|                                 |                                            |
|---------------------------------|--------------------------------------------|
| <a href="#">no</a> on page 1114 | Removes the fallback-channel configuration |
|---------------------------------|--------------------------------------------|

guard-interval

[interface-config-radio-instance](#) on page 1072

Configures the 802.11n guard interval. A guard interval ensures distinct transmissions do not interfere with one another. It provides immunity to propagation delays, echoes and reflection of radio signals.

The guard interval is the space between transmitted characters. The guard interval eliminates inter symbol interference (ISI). ISI which occurs when echoes or reflections from one symbol interferes with another. Adding time between transmissions allows echoes and reflections to settle before the next symbol is transmitted. A shorter guard interval results in shorter symbol times, which reduces overhead and increases data rates by up to 10%.

Supported in the following platforms:

- Access Points – AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

Syntax

```
guard-interval [any|long]
```

Parameters

```
guard-interval [any|long]
```



|                       |                                                                                |
|-----------------------|--------------------------------------------------------------------------------|
| <b>guard-interval</b> | Configures the 802.11n guard interval                                          |
| <b>any</b>            | Enables the radio to use any short (400nSec) or long (800nSec) guard interval  |
| <b>long</b>           | Enables the use of long guard interval (800nSec). This is the default setting. |

### Example

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#guard-interval long
```

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#show context
interface radiol
 description "Primary radio to use"
 channel 1
 data-rates b-only
 beacon period 50
 beacon dtim-period bss 1 5
 beacon dtim-period bss 2 2
 beacon dtim-period bss 3 5
 beacon dtim-period bss 4 5
 beacon dtim-period bss 5 5
 beacon dtim-period bss 6 5
 beacon dtim-period bss 7 5
 beacon dtim-period bss 8 5
 beacon dtim-period bss 9 5
 beacon dtim-period bss 10 5
 beacon dtim-period bss 11 5
 beacon dtim-period bss 12 5
 beacon dtim-period bss 13 5
 beacon dtim-period bss 14 5
 beacon dtim-period bss 15 5
 beacon dtim-period bss 16 5
 antenna-gain 12.0
 guard-interval long
--More--
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#
```

### Related Commands

|                        |                                                              |
|------------------------|--------------------------------------------------------------|
| <b>no</b> on page 1114 | Resets the 802.11n guard interval to default (long: 800nSec) |
|------------------------|--------------------------------------------------------------|

### ldpc

[interface-config-radio-instance](#) on page 1072

Enables support for Low Density Parity Check (LDPC) codes on the radio interface

LDPC consists of forward error correcting codes that enable error control in data transmission. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

Syntax

`ldpc`

Parameters

None

### Example

```
rfs4000-229D58(config-profile-Test81XX-if-radiol)#ldpc

rfs4000-229D58(config-profile-Test81XX-if-radiol)#show context
 interface radiol
 ldpc
rfs4000-229D58(config-profile-Test81XX-if-radiol)#
```

### Related Commands

|                                 |                       |
|---------------------------------|-----------------------|
| <a href="#">no</a> on page 1114 | Disables LDPC support |
|---------------------------------|-----------------------|

### lock-rf-mode

[interface-config-radio-instance](#) on page 1072

Retains user configured RF mode settings for the selected radio. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

### Syntax

```
lock-rf-mode
```

### Parameters

None

### Example

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#lock-rf-mode

nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#show context
 interface radiol
 description "Primary radio to use"
 channel 1
 data-rates b-only
 beacon period 50
 beacon dtim-period bss 1 5
 beacon dtim-period bss 2 2
 beacon dtim-period bss 3 5
 beacon dtim-period bss 4 5
 beacon dtim-period bss 5 5
 beacon dtim-period bss 6 5
 beacon dtim-period bss 7 5
 beacon dtim-period bss 8 5
 beacon dtim-period bss 9 5
 beacon dtim-period bss 10 5
 beacon dtim-period bss 11 5
 beacon dtim-period bss 12 5
 beacon dtim-period bss 13 5
 beacon dtim-period bss 14 5
 beacon dtim-period bss 15 5
 beacon dtim-period bss 16 5
 antenna-gain 12.0
 guard-interval long
 aggregation ampdu tx-only
 aeroscout forward
 ekahau forward ip 172.16.10.1 port 3
 antenna-mode 2x2
 antenna-diversity
```

```

airtime-fairness prefer-ht weight 6
lock-rf-mode
extended-range 15
--More--
nx9500-6C8809(config-profile-7lxxTestProfile-if-radio1)#

```

#### Related Commands

|                                 |                                                      |
|---------------------------------|------------------------------------------------------|
| <a href="#">no</a> on page 1114 | Allows Smart RF to change a radio's RF mode settings |
|---------------------------------|------------------------------------------------------|

#### max-clients

[interface-config-radio-instance](#) on page 1072

Configures the maximum number of wireless clients allowed to associate with this radio

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

#### Syntax

```
max-clients <0-256>
```

#### Parameters

```
max-clients <0-256>
```

|                                            |                                                                                                                                                                    |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>max-clients</b><br><b>&lt;0-256&gt;</b> | Configures the maximum number of clients allowed to associate with a radio, subject to the access point's limit. Specify a value from 0 - 256. The default is 256. |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Example

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radio1)#max-clients 100
```

```

nx9500-6C8809(config-profile-7lxxTestProfile-if-radio1)#show context
interface radiol
description "Primary radio to use"
channel 1
data-rates b-only
beacon period 50
beacon dtim-period bss 1 5
beacon dtim-period bss 2 2
.....
beacon dtim-period bss 12 5
beacon dtim-period bss 13 5
beacon dtim-period bss 14 5
beacon dtim-period bss 15 5
beacon dtim-period bss 16 5
antenna-gain 12.0
guard-interval long
aggregation ampdu tx-only
aeroscout forward
ekahau forward ip 172.16.10.1 port 3
antenna-mode 2x2
antenna-diversity
max-clients 100
airtime-fairness prefer-ht weight 6
lock-rf-mode
extended-range 15
antenna-downtilt
nx9500-6C8809(config-profile-7lxxTestProfile-if-radio1)#

```

#### Related Commands

mesh

[interface-config-radio-instance](#) on page 1072

Use this command to configure radio mesh parameters. A Wireless Mesh Network (WMN) is a network of radio nodes organized in a mesh topology. It consists of mesh clients, mesh routers, and gateways.

Each radio setting can have a unique mesh mode and link configuration. This provides a customizable set of connections to other mesh supported radios within the same radio coverage area.

Supported in the following platforms:

- Access Points – AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP8163, AP8432, AP8533

Syntax

```
mesh [client|links|portal|preferred-peer|psk]
```

```
mesh [client|links <1-6>|portal|preferred-peer <1-6> <MAC>|psk [0 <LINE>|2 <LINE>| <LINE>]]
```

Parameters

```
mesh [client|links <1-6>|portal|preferred-peer <1-6> <MAC>|psk [0 <LINE>|2 <LINE>|<LINE>]]
```

|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mesh</b>                                             | Configures radio mesh parameters, such as maximum number of mesh links, preferred peer device, client operations, etc.                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>client</b>                                           | Enables operation as a client<br>Setting the mesh mode to 'client' enables the radio to operate as a mesh client that scans for and connects to mesh portals or nodes that are connected to portals.                                                                                                                                                                                                                                                                                                                 |
| <b>links &lt;1-6&gt;</b>                                | Configures the maximum number of mesh links a radio attempts to create <ul style="list-style-type: none"> <li>• &lt;1-6&gt; - Sets the maximum number of mesh links from 1 - 6. The default is 6.</li> </ul>                                                                                                                                                                                                                                                                                                         |
| <b>portal</b>                                           | Enables operation as a portal<br>Setting the mesh mode to 'portal' turns the radio into a mesh portal. The radio starts beaconing immediately and accepts connections from other mesh nodes, typically the node with a connection to the wired network.                                                                                                                                                                                                                                                              |
| <b>preferred-peer &lt;1-6&gt; &lt;MAC&gt;</b>           | Configures a preferred peer device <ul style="list-style-type: none"> <li>• &lt;1-6&gt; - Configures the priority at which the peer node will be added</li> </ul> <p>When connecting to the mesh infrastructure, nodes with lower priority are given precedence over nodes with higher priority.</p> <ul style="list-style-type: none"> <li>• &lt;MAC&gt; - Sets the MAC address of the preferred peer device (Ethernet MAC of either a AP, wireless controller, or service platform with onboard radios)</li> </ul> |
| <b>psk [0 &lt;LINE&gt; 2 &lt;LINE&gt; &lt;LINE&gt;]</b> | Configures the pre-shared key. Ensure this key is configured on the access point when staged for mesh, and added to the mesh client and to the portal access point's configuration on the controller or service platform. <ul style="list-style-type: none"> <li>• 0 &lt;LINE&gt; - Enter a clear text key</li> <li>• 2 &lt;LINE&gt; - Enter an encrypted key</li> <li>• &lt;LINE&gt; - Enter the pre-shared key</li> </ul> <p>Pre-shared keys should be 8 - 64 characters in length.</p>                            |

### Example

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#mesh client

nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#show context
interface radiol
 description "Primary radio to use"
 channel 1
 data-rates b-only
 mesh client
 beacon period 50
 --More--
nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#
```

### Related Commands

|                                 |                                                    |
|---------------------------------|----------------------------------------------------|
| <a href="#">no</a> on page 1114 | Disables mesh mode operation of the selected radio |
|---------------------------------|----------------------------------------------------|

## meshpoint

[interface-config-radio-instance](#) on page 1072

Maps an existing meshpoint to this radio

Use this command to assign each WLAN its own BSSID. If using a single-radio access point, there are 8 BSSIDs available. If using a dual-radio access point there are 8 BSSIDs for the 802.11b/g/n radio and 8 BSSIDs for the 802.11a/n radio.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP8163, AP8432, AP8533

### Syntax

```
meshpoint <MESHPOINT-NAME> {bss <1-16>}
```

### Parameters

```
meshpoint <MESHPOINT-NAME> {bss <1-16>}
```

|                                                   |                                                                                                                                                                         |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>meshpoint</b><br><b>&lt;MESHPOINT-NAME&gt;</b> | Maps a meshpoint to this radio. Specify the meshpoint name.                                                                                                             |
| <b>bss &lt;1-16&gt;</b>                           | Optional. Specifies the radio's BSS where this meshpoint is mapped <ul style="list-style-type: none"><li>• &lt;1-16&gt; - Specify the BSS number from 1 - 16.</li></ul> |

### Example

```
nx9500-6C8809(config-profile-ap71xxTest-if-radiol)#meshpoint test bss 7
nx9500-6C8809(config-profile-ap71xxTest-if-radiol)#show context
interface radiol
 meshpoint test bss 7
nx9500-6C8809(config-profile-ap71xxTest-radiol)#
```

### Related Commands

|                                 |                                          |
|---------------------------------|------------------------------------------|
| <a href="#">no</a> on page 1114 | Disables meshpoint on the selected radio |
|---------------------------------|------------------------------------------|

## mu-mimo

[interface-config-radio-instance](#) on page 1072

Enables multi-user multiple input multiple output (MU-MIMO) support on the selected radio. When enabled, multiple users are able to simultaneously access the same channel using the spatial degrees of freedom offered by MIMO.

Supported in the following platforms:

- Access Points — AP7532, AP7562, AP8163, AP8432, AP8533

Syntax

```
mu-mimo
```

Parameters

None

Example

```
nx9500-6C8809(config-profile-TestAP81xx-if-radio1)#mu-mimo
nx9500-6C8809(config-profile-TestAP81xx-if-radio1)#show context include-factory | include
mu-mimo
 mu-mimo
nx9500-6C8809(config-profile-TestAP81xx-if-radio1)#
```

```
ap7532-80C2AC(config-device-84-24-8D-80-C2-AC-if-radio1)#mu-mimo
```

```
ap7532-80C2AC(config-device-84-24-8D-80-C2-AC-if-radio1)#show context include-factory |
include mu-mimo
 mu-mimo
ap7532-80C2AC(config-device-84-24-8D-80-C2-AC-if-radio1)#
```

Related Commands

|                              |                                        |
|------------------------------|----------------------------------------|
| <code>no</code> on page 1114 | Disables mu-mimo on the selected radio |
|------------------------------|----------------------------------------|

no

[interface-config-radio-instance](#) on page 1072

Negates a command or resets settings to their default. When used in the profile/device > radio interface configuration mode, the no command disables or resets radio interface settings.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

Syntax

```
no <PARAMETERS>
```

Parameters

```
no <PARAMETERS>
```

|                                        |                                                                                   |
|----------------------------------------|-----------------------------------------------------------------------------------|
| <b>no</b><br><b>&lt;PARAMETERS&gt;</b> | Removes or reverts this radio interface's settings based on the parameters passed |
|----------------------------------------|-----------------------------------------------------------------------------------|

Usage Guidelines

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

## Example

```
nx9500-6C8809(config-profile-ap71xxTest-if-radiol)#no ?
 adaptivity Adaptivity
 aeroscout Use Default Aeroscout Multicast MAC Address
 aggregation Configure 802.11n aggregation related parameters
 airtime-fairness Disable fair access to medium for clients,
 provide access in a round-robin mode
 antenna-diversity Use single antenna for non-11n transmit rates
 antenna-downtilt Reset ADEPT antenna mode
 antenna-elevation Reset the antenna elevation of this radio to
 default
 antenna-gain Reset the antenna gain of this radio to default
 antenna-mode Reset the antenna mode (number of transmit and
 receive antennas) on the radio to its default
 assoc-response Configure transmission parameters for
 Association Response frames
 association-list Configure the association list for the radio
 beacon Configure beacon parameters
 bridge Bridge rf-mode related configuration
 channel Reset the channel of operation of this radio to
 default
 data-rates Reset radio data rate configuration to default
 description Reset the description of the radio to its
 default
 dfs-rehome Stay on dfs elected channel after evacuation
 period expires
 dynamic-chain-selection Use the configured transmit antenna mode for all
 clients
 ekahau Use Default Ekahau Multicast MAC Address
 extended-range Reset extended range to default
 fallback-channel Clear the DFS fallback channel for this radio
 guard-interval Configure default value of 802.11n guard
 interval (long: 800nSec)
 ldpc Configure support for Low Density Parity Check
 Code
 lock-rf-mode Allow smart-rf to change rf-mode setting for
 this radio
 max-clients Maximum number of wireless clients allowed to
 associate
 mesh Disable mesh mode operation of the radio
 meshpoint Disable a meshpoint from this radio
 mu-mimo Disable multi user MIMO on this radio (selected
 platforms only)
 non-unicast Configure handling of non-unicast frames
 off-channel-scan Disable off-channel scanning on the radio
 placement Reset the placement of the radio to its default
 power Reset the transmit power of this radio to
 default
 preamble-short Disable the use of short-preamble on this radio
 probe-response Configure transmission parameters for Probe
 Response frames
 radio-resource-measurement Configure support for 802.11k Radio Resource
 Measurement
 radio-share-mode Configure the radio-share mode of operation for
 this radio
 rate-selection Monotonic rate selection
 rf-mode Reset the RF mode of operation for this radio to
 default (2.4GHz on radiol, 5GHz on radio2,
 sensor on radio3)
 rifs Configure Reduced Interframe Spacing (RIFS)
 parameters
 rts-threshold Reset the RTS threshold to its default (65536)
 shutdown Re-enable the selected interface
 smart-rf Reset smart-rf related configuration to default
```

|                      |                                                     |
|----------------------|-----------------------------------------------------|
| sniffer-redirect     | Disable capture and redirection of packets          |
| stbc                 | Configure Space-Time Block Coding (STBC) parameters |
| transmit-beamforming | Disable Transmit Beamforming                        |
| use                  | Set setting to use                                  |
| wips                 | Wireless intrusion prevention related configuration |
| wireless-client      | Configure wireless client related parameters        |
| wlan                 | Disable a wlan from this radio                      |
| service              | Service Commands                                    |

```
nx9500-6C8809(config-profile-ap7lxxTest-if-radiol)#
```

The following example shows radio interface settings before the 'no' commands are executed:

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#show context
interface radiol
 description "Primary radio to use"
 channel 1
 data-rates b-only
 mesh client
 beacon period 50
 beacon dtim-period bss 1 5
 beacon dtim-period bss 2 2
 beacon dtim-period bss 3 5
 beacon dtim-period bss 4 5
 beacon dtim-period bss 5 5
 beacon dtim-period bss 6 5
 beacon dtim-period bss 7 5
 beacon dtim-period bss 8 5
 beacon dtim-period bss 9 5
 beacon dtim-period bss 10 5
 beacon dtim-period bss 11 5
 beacon dtim-period bss 12 5
 beacon dtim-period bss 13 5
 beacon dtim-period bss 14 5
 beacon dtim-period bss 15 5
 beacon dtim-period bss 16 5
 antenna-gain 12.0
 guard-interval long
 aggregation ampdu tx-only
 aeroscout forward
 ekahau forward ip 172.16.10.1 port 3
 antenna-mode 2x2
 antenna-diversity
 max-clients 100
 airtime-fairness prefer-ht weight 6
 lock-rf-mode
 extended-range 15
 antenna-downtilt
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#
```

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#no channel
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#no antenna-gain
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#no description
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#no antenna-mode
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#no beacon dtim-period
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#no beacon period
```

The following example shows radio interface settings after the 'no' commands are executed:

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#show context
interface radiol
 data-rates b-only
```



```

mesh client
guard-interval long
aggregation ampdu tx-only
aeroscout forward
ekahau forward ip 172.16.10.1 port 3
antenna-diversity
max-clients 100
airtime-fairness prefer-ht weight 6
lock-rf-mode
extended-range 15
antenna-downtilt
nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#
non-unicast

```

[interface-config-radio-instance](#) on page 1072

Configures support for forwarding of non-unicast (multicast and broadcast) frames on this radio

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

Syntax

```
non-unicast [forwarding|queue|tx-rate]
```

```
non-unicast forwarding [follow-dtim|power-save-aware]
```

```
non-unicast queue [<1-200>|bss]
```

```
non-unicast queue [<1-200>|bss <1-16> <1-200>]
```

```
non-unicast tx-rate [bss <1-16>|dynamic-all|dynamic-basic|highest-basic|lowest-basic]
```

```
non-unicast tx-rate bss <1-16> [dynamic-all|dynamic-basic|highest-basic|lowest-basic]
```

Parameters

```
non-unicast forwarding [follow-dtim|power-save-aware]
```

|                               |                                                                                                                                                                                                                        |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>non-unicast forwarding</b> | Enables non-unicast frame forwarding on this radio. Once enabled, select one of the available options to specify whether these frames should always follow DTIM, or only follow DTIM when using power save aware mode. |
| <b>follow-dtim</b>            | Specifies frames always wait for the DTIM interval to time out. The DTIM interval is configured using the beacon command. This is the default setting.                                                                 |
| <b>power-save-aware</b>       | Enables immediate forwarding of frames only if all associated wireless clients are in the power save mode                                                                                                              |

```
non-unicast queue [<1-200>|bss <1-16> <1-200>]
```

|                                           |                                                                                                                                                                                                                                                             |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>non-unicast queue</b>                  | Enables non-unicast frame forwarding on this radio. Once enabled, specify the number of broadcast packets queued per BSS on this radio. This option is enabled by default. This command also enables you to override the default on a specific BSS.         |
| <b>&lt;1-200&gt;</b>                      | Specify a number from 1 - 200. This value applies to all BSSs. The default is 50 frames per BSS.                                                                                                                                                            |
| <b>bss &lt;1-16&gt;<br/>&lt;1-200&gt;</b> | Overrides the default on a specified BSS <ul style="list-style-type: none"> <li>• &lt;1-16&gt; - Select the BSS number from 1 - 16.</li> <li>• &lt;1-200&gt; - Specify the number of broadcast packets queued for the selected BSS from 1 - 200.</li> </ul> |

non-unicast tx-rate [bss <1-16>|dynamic-all|dynamic-basic|highest-basic| lowest-basic]

|                            |                                                                                                                                                                                                                                                                                                        |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>non-unicast tx-rate</b> | Enables non-unicast frame forwarding on this radio. Once enabled, use one of the available options to configure the rate at which these frames are transmitted.                                                                                                                                        |
| <b>bss &lt;1-16&gt;</b>    | Overrides the default on a specified BSS <ul style="list-style-type: none"> <li>• &lt;1-16&gt; - Select the BSS number from 1 - 16. The transmit rate selected is applied only to the BSS specified here. The tx-rate options are: dynamic-all, dynamic-basic, highest-basic, lowest-basic.</li> </ul> |
| <b>dynamic-all</b>         | Dynamically selects a rate from all supported rates based on current traffic conditions                                                                                                                                                                                                                |
| <b>dynamic-basic</b>       | Dynamically selects a rate from all supported basic rates based on current traffic conditions                                                                                                                                                                                                          |
| <b>highest-basic</b>       | Uses the highest configured basic rate. This is the default setting.                                                                                                                                                                                                                                   |
| <b>lowest-basic</b>        | Uses the lowest configured basic rate                                                                                                                                                                                                                                                                  |

#### Example

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#non-unicast queue bss 2 3
```

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#non-unicast tx-rate bss 1 dynamic-all
```

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#show context
interface radiol
 data-rates b-only
 mesh client
 guard-interval long
 aggregation ampdu tx-only
 aeroscout forward
 ekahau forward ip 172.16.10.1 port 3
 non-unicast tx-rate bss 1 dynamic-all
 non-unicast tx-rate bss 2 highest-basic
 non-unicast tx-rate bss 3 highest-basic
 non-unicast tx-rate bss 4 highest-basic
 non-unicast tx-rate bss 5 highest-basic
 non-unicast tx-rate bss 6 highest-basic
 non-unicast tx-rate bss 7 highest-basic
 non-unicast tx-rate bss 8 highest-basic
 non-unicast tx-rate bss 9 highest-basic
 non-unicast tx-rate bss 10 highest-basic
 non-unicast tx-rate bss 11 highest-basic
 non-unicast tx-rate bss 12 highest-basic
 non-unicast tx-rate bss 13 highest-basic
 non-unicast tx-rate bss 14 highest-basic
 non-unicast tx-rate bss 15 highest-basic
 non-unicast tx-rate bss 16 highest-basic
```

```

non-unicast queue bss 1 50
non-unicast queue bss 2 3
--More--
antenna-diversity
max-clients 100
airtime-fairness prefer-ht weight 6
lock-rf-mode
extended-range 15
antenna-downtilt
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#

```

#### Related Commands

|                                 |                                                          |
|---------------------------------|----------------------------------------------------------|
| <a href="#">no</a> on page 1114 | Resets the handling of non-unicast frames to its default |
|---------------------------------|----------------------------------------------------------|

#### off-channel-scan

[interface-config-radio-instance](#) on page 1072

Enables off channel scanning on this radio. This option is disabled by default.

Channel scanning uses the access point's resources and is time consuming. Therefore, enable this option only if the radio has the bandwidth to support channel scan without negatively impacting client support.

Supported in the following platforms:

- Access Points – AP6522, AP6562, AP7161, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

#### Syntax

```
off-channel-scan {channel-list|max-multicast|scan-interval|sniffer-redirect}
```

```
off-channel-scan {channel-list [2.4Ghz|5Ghz]} {<CHANNEL-LIST>}
```

```
off-channel-scan {max-multicast <0-100>|scan-interval <2-100>}
```

```
off-channel-scan {sniffer-redirect tzsp <IP>}
```

#### Parameters

```
off-channel-scan {channel-list [2.4Ghz|5Ghz]} {<CHANNEL-LIST>}
```

|                                     |                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>off-channel-scan</b>             | Enables off-channel scanning and configures related parameters. These parameters are optional, and the system configures default settings if no values are specified.                                                                                                                                                  |
| <b>channel-list [2.4GHz   5GHz]</b> | Optional. Selects the 2.4GHz or 5GHz access point radio band. Restricting off channel scans to specific channels frees bandwidth otherwise utilized for scanning across all channels. <ul style="list-style-type: none"> <li>• 2.4GHz – Selects the 2.4 GHz band</li> <li>• 5GHz – Selects the 5.0 GHz band</li> </ul> |
| <b>&lt;CHANNEL-LIST&gt;</b>         | Optional. Specifies a list of 20 MHz, 40 MHz, or 80 MHz channels for the selected band (the channels are separated by commas or hyphens)                                                                                                                                                                               |

```
off-channel-scan {max-multicast <0-100>|scan-interval <2-100>}
```

|                                              |                                                                                                                                                                                                       |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>off-channel-scan</b>                      | Enables off-channel scanning and configures related parameters. These parameters are optional, and the system configures default settings if no values are specified.                                 |
| <b>max-multicast</b><br><b>&lt;0-100&gt;</b> | Optional. Configures the maximum multicast/broadcast messages used to perform OCS <ul style="list-style-type: none"> <li>• &lt;0-100&gt; - Specify a value from 0 - 100. The default is 4.</li> </ul> |
| <b>scan-interval</b><br><b>&lt;2-100&gt;</b> | Optional. Configures the scan interval in dtims <ul style="list-style-type: none"> <li>• &lt;2-100&gt; - Specify a value from 2 - 100. The default is 20 dtims.</li> </ul>                            |

```
off-channel-scan {sniffer-redirect tzsp <IP>}
```

|                                                   |                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>off-channel-scan</b>                           | Enables off-channel scanning and configures related parameters. These parameters are optional, and the system configures default settings if no values are specified.                                                                                                                                                                                             |
| <b>sniffer-redirect</b><br><b>tzsp &lt;IP&gt;</b> | Optional. Captures and redirects packets to a host running a packet capture/analysis tool. Use this command to configure the IP address of the host. <ul style="list-style-type: none"> <li>• tzsp - Encapsulates captured packets in TZSP before redirecting to the specified host</li> <li>• &lt;IP&gt; - Specify the destination device IP address.</li> </ul> |

#### Example

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radio1)#off-channel-scan channel-list 2.4GHz 1
```

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radio1)#show context
interface radio1
 data-rates b-only
 mesh client
 off-channel-scan channel-list 2.4GHz 1
 guard-interval long
 aggregation ampdu tx-only
 aeroscout forward
 ekahau forward ip 172.16.10.1 port 3
 non-unicast tx-rate bss 1 dynamic-all
 non-unicast tx-rate bss 2 highest-basic
 non-unicast tx-rate bss 3 highest-basic
 non-unicast tx-rate bss 4 highest-basic
 non-unicast tx-rate bss 5 highest-basic
 non-unicast tx-rate bss 6 highest-basic
 non-unicast tx-rate bss 7 highest-basic
 non-unicast tx-rate bss 8 highest-basic
 non-unicast tx-rate bss 9 highest-basic
 non-unicast tx-rate bss 10 highest-basic
 non-unicast tx-rate bss 11 highest-basic
 non-unicast tx-rate bss 12 highest-basic
 non-unicast tx-rate bss 13 highest-basic
 non-unicast tx-rate bss 14 highest-basic
 non-unicast tx-rate bss 15 highest-basic
--More--
nx9500-6C8809(config-profile-7lxxTestProfile-if-radio1)#
```

#### Related Commands

|                                 |                                     |
|---------------------------------|-------------------------------------|
| <a href="#">no</a> on page 1114 | Disables radio off channel scanning |
|---------------------------------|-------------------------------------|

placement

[interface-config-radio-instance](#) on page 1072

Defines the radio's location (whether the radio is deployed indoors or outdoors). The radio's placement should depend on the country of operation selected and its regulatory domain requirements for radio emissions.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

Syntax

`placement [ indoor|outdoor ]`

Parameters

`placement [ indoor|outdoor ]`

|                  |                                                                                        |
|------------------|----------------------------------------------------------------------------------------|
| <b>placement</b> | Defines the radio's location                                                           |
| <b>indoor</b>    | Radio is deployed indoors (uses indoor regulatory rules). This is the default setting. |
| <b>outdoor</b>   | Radio is deployed outdoors (uses outdoor regulatory rules)                             |

Example

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#placement outdoor
```

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#show context
```

```
interface radiol
 data-rates b-only
 placement outdoor
 mesh client
 off-channel-scan channel-list 2.4GHz 1
 guard-interval long
 aggregation ampdu tx-only
 aeroscout forward
 ekahau forward ip 172.16.10.1 port 3
 non-unicast tx-rate bss 1 dynamic-all
 non-unicast tx-rate bss 2 highest-basic
 non-unicast tx-rate bss 3 highest-basic
 non-unicast tx-rate bss 4 highest-basic
 non-unicast tx-rate bss 5 highest-basic
 non-unicast tx-rate bss 6 highest-basic
 non-unicast tx-rate bss 7 highest-basic
 non-unicast tx-rate bss 8 highest-basic
 non-unicast tx-rate bss 9 highest-basic
 non-unicast tx-rate bss 10 highest-basic
 non-unicast tx-rate bss 11 highest-basic
 non-unicast tx-rate bss 12 highest-basic
 non-unicast tx-rate bss 13 highest-basic
 non-unicast tx-rate bss 14 highest-basic
```

--More--

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#
```

Related Commands

|                              |                                      |
|------------------------------|--------------------------------------|
| <code>no</code> on page 1114 | Resets a radio's deployment location |
|------------------------------|--------------------------------------|

power

`interface-config-radio-instance` on page 1072

Configures the radio's transmit power setting

The transmit power control (TPC) mechanism automatically reduces the used transmission output power when other networks are within range. Reduced power results in reduced interference issues and increased battery capacity.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

Syntax

```
power [<1-30>|smart]
```

Parameters

```
power [<1-30>|smart]
```

|                     |                                                                                                                                                                                                                                                                     |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>power</b>        | Configures a radio's transmit power                                                                                                                                                                                                                                 |
| <b>&lt;1-30&gt;</b> | Configures the transmit power from 1 - 30 dBm (actual power could be lower based on regulatory restrictions)<br>For APs with dual or three radios, each radio should be configured with a unique transmit power in respect to its intended client support function. |
| <b>smart</b>        | Enables Smart RF to determine the optimum transmit power needed. By default APs use Smart RF to determine transmit power.                                                                                                                                           |

Example

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#power 12
```

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#show context
```

```
interface radiol
 power 12
 data-rates b-only
 placement outdoor
 mesh client
 off-channel-scan channel-list 2.4GHz 1
 guard-interval long
 aggregation ampdu tx-only
 aeroscout forward
 ekahau forward ip 172.16.10.1 port 3
 non-unicast tx-rate bss 1 dynamic-all
 non-unicast tx-rate bss 2 highest-basic
 non-unicast tx-rate bss 3 highest-basic
 non-unicast tx-rate bss 4 highest-basic
 non-unicast tx-rate bss 5 highest-basic
 non-unicast tx-rate bss 6 highest-basic
 non-unicast tx-rate bss 7 highest-basic
```

--More--

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#
```

Related Commands

|                                 |                                 |
|---------------------------------|---------------------------------|
| <a href="#">no</a> on page 1114 | Resets a radio's transmit power |
|---------------------------------|---------------------------------|

[preamble-short](#)

[interface-config-radio-instance](#) on page 1072

Enables short preamble on this radio. If using an 802.11bg radio, enable short preamble. Short preambles improve throughput. However, some devices (SpectralLink phones) require long preambles. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP8163, AP8432, AP8533

Syntax

`preamble-short`

Parameters

None

Example

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#preamble-short
```

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#show context
interface radiol
 power 12
 data-rates b-only
 placement outdoor
 mesh client
 off-channel-scan channel-list 2.4GHz 1
 preamble-short
 guard-interval long
 aggregation ampdu tx-only
 aeroscout forward
 ekahau forward ip 172.16.10.1 port 3
 non-unicast tx-rate bss 1 dynamic-all
 non-unicast tx-rate bss 2 highest-basic
 non-unicast tx-rate bss 3 highest-basic
 non-unicast tx-rate bss 4 highest-basic
 non-unicast tx-rate bss 5 highest-basic
 non-unicast tx-rate bss 6 highest-basic
 non-unicast tx-rate bss 7 highest-basic
 non-unicast tx-rate bss 8 highest-basic
 non-unicast tx-rate bss 9 highest-basic
 non-unicast tx-rate bss 10 highest-basic
 non-unicast tx-rate bss 11 highest-basic
 non-unicast tx-rate bss 12 highest-basic
--More--
nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#
```

Related Commands

|                                 |                                               |
|---------------------------------|-----------------------------------------------|
| <a href="#">no</a> on page 1114 | Disables the use of short preamble on a radio |
|---------------------------------|-----------------------------------------------|

probe-response

[interface-config-radio-instance](#) on page 1072

Configures transmission parameters for probe response frames

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

Syntax

```
probe-response [rate|retry|rssi-threshold]
```

```
probe-response retry
```

```
probe-response rate [follow-probe-request|highest-basic|lowest-basic]
```

```
probe-response rssi-threshold <-128--40>
```

Parameters

```
probe-response retry
```

|                                 |                                                                                                                                       |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <b>probe-response<br/>retry</b> | Enables retransmission of probe-response frames if no acknowledgement is received from the client. This option is enabled by default. |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|

```
probe-response rate [follow-probe-request|highest-basic|lowest-basic]
```

|                                  |                                                                                                                                                                                                   |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>probe-response<br/>rate</b>   | Configures the rates used for transmission of probe response frames. The tx-rate options available for transmitting probe response frames are: follow-probe-request, highest-basic, lowest-basic. |
| <b>follow-probe-<br/>request</b> | Transmits probe responses at the same rate as the received request (default setting)                                                                                                              |
| <b>highest-basic</b>             | Uses the highest configured basic rate                                                                                                                                                            |
| <b>lowest-basic</b>              | Uses the lowest configured basic rate                                                                                                                                                             |

```
probe-response rssi-threshold <-128--40>
```

|                                                               |                                                                                                                                                                   |
|---------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>probe-response<br/>rssi-threshold<br/>&lt;-128--40&gt;</b> | Ignores probe request from client if the received signal strength is less than the RSSI threshold specified here<br><-128--40> - Specify a value from -128 - -40. |
|---------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Example

```
nx9500-6C8809(config-profile-testAP7161-if-radio1)#probe-response rate highest-basic
```

```
nx9500-6C8809(config-profile-testAP7161-if-radio1)#probe-response retry
```

```
nx9500-6C8809(config-profile-testAP7161-if-radio1)#probe-response rssi-threshold -60
```

```
nx9500-6C8809(config-profile-testAP7161-if-radio1)#show context
```

```
interface radio1
```

```
 probe-response rate highest-basic
```

```
 probe-response rssi-threshold -60
```

```
nx9500-6C8809(config-profile-testAP7161-if-radio1)#
```

Related Commands

|                                 |                                                          |
|---------------------------------|----------------------------------------------------------|
| <a href="#">no</a> on page 1114 | Resets transmission parameters for probe response frames |
|---------------------------------|----------------------------------------------------------|

radio-resource-measurement

[interface-config-radio-instance](#) on page 1072

Enables 802.11k radio resource measurement. When enabled, the radio station sends channel and neighbor reports.



The IEEE 802.11 Task Group k defined a set of specifications regarding radio resource measurements. These specifications specify the radio resources to be measured and the mechanism used to communicate measurement requests and results.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

Syntax

```
radio-resource-measurement [attenuation-threshold <1-199>|max-entries <1-12>]
```

Parameters

```
radio-resource-measurement [attenuation-threshold <1-199>|max-entries <1-12>]
```

|                                            |                                                                                                                                                                                                                                            |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>radio-resource-measurement</b>          | Enables 802.11k radio resource measurement on the radio                                                                                                                                                                                    |
| <b>attenuation-threshold &lt;1-199&gt;</b> | Configures the neighbor attenuation threshold, considered when generating channel and neighbor reports <ul style="list-style-type: none"><li>• &lt;1-199&gt; - Specify the attenuation threshold from 1 -199. The default is 90.</li></ul> |
| <b>max-entries &lt;1-12&gt;</b>            | Configures the maximum number of entries to include in channel and neighbor reports <ul style="list-style-type: none"><li>• &lt;1-12&gt; - Specify a value from 1 - 12. The default is 6.</li></ul>                                        |

Example

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-if-radiol)#radio-resource-measurement attenuation-threshold 20
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-if-radiol)#radio-resource-measurement max-entries 10
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-if-radiol)#show context interface radiol radio-resource-measurement max-entries 10 radio-resource-measurement attenuation-threshold 20 rfs4000-229D58(config-device-00-23-68-22-9D-58-if-radiol)#
```

Related Commands

|                                 |                                                     |
|---------------------------------|-----------------------------------------------------|
| <a href="#">no</a> on page 1114 | Disables 802.11k radio resource measurement support |
|---------------------------------|-----------------------------------------------------|

radio-share-mode

[interface-config-radio-instance](#) on page 1072

Configures the radio's mode of operation as radio share. A radio operating in the radio share mode services clients and also performs sensor functions (defined by the radio's AirDefense Services Platform (ADSP) licenses and profiles).



**Note**

The sensor capabilities of the radio are restricted to the channel and WLANs defined on the radio.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP8163, AP8432, AP8533

Syntax

`radio-share-mode [inline|off|promiscuous]`

Parameters

`radio-share-mode [inline|off|promiscuous]`

|                         |                                                                                                                                                                                                                                                                                                     |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>radio-share-mode</b> | Enables sharing of packets, switched by this radio, with the WIPS sensor module. There are two radio-share modes, these are: inline and promiscuous                                                                                                                                                 |
| <b>inline</b>           | Enables sharing of all WLAN packets (matching the BSSID of the radio) serviced by the radio with the WIPS sensor module.                                                                                                                                                                            |
| <b>off</b>              | Disables radio share (no packets shared with the WIPS sensor module)                                                                                                                                                                                                                                |
| <b>promiscuous</b>      | Enables the promiscuous radio share mode. In this mode the radio is configured to receive all packets on the channel irrespective of whether the destination address is the radio or not, and shares these packets with the WIPS sensor module for analysis (i.e. without filtering based on BSSI). |

Example

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#radio-share-mode promiscuous
```

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#show context
interface radiol
 power 12
 data-rates b-only
 placement outdoor
 mesh client
 off-channel-scan channel-list 2.4GHz 1
 preamble-short
 guard-interval long

 non-unicast queue bss 16 50
 antenna-diversity
 max-clients 100
 radio-share-mode promiscuous
 airtime-fairness prefer-ht weight 6
 lock-rf-mode
 extended-range 15
 antenna-downtilt
nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#
```

Related Commands

|                                 |                                                           |
|---------------------------------|-----------------------------------------------------------|
| <a href="#">no</a> on page 1114 | Resets the radio share mode for this radio to its default |
|---------------------------------|-----------------------------------------------------------|

rate-selection

[interface-config-radio-instance](#) on page 1072

Sets the data-rate selection mode to standard or opportunistic

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

Syntax

```
rate-selection [opportunistic|standard]
```

Parameters

```
rate-selection [opportunistic|standard]
```

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>rate-selection</b> | Sets the rate selection mode to standard or opportunistic                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>standard</b>       | Configures the monotonic rate selection mode. This is the default setting.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>opportunistic</b>  | Configures the opportunistic radio link adaptation (ORLA) rate selection mode. The ORLA algorithm is designed to select data rates that provide best throughput. Instead of using local conditions to decide whether a data rate is acceptable or not, ORLA pro-actively probes other rates to determine if greater throughput is available. If these other rates do provide improved throughput, ORLA intelligently adjusts its selection tables to favour higher performance. ORLA provides improvements both on the client side of a mesh network as well as in the backhaul capabilities.<br><br><b>Note:</b> The ORLA rate selection mode is supported only on the AP7161 and AP8163 model access points. |

Example

```
nx9500-6C8809(config-profile-testAP7161-if-radiol)#rate-selection opportunistic
```

```
nx9500-6C8809(config-profile-testAP7161-if-radiol)#show context
interface radiol
 rate-selection opportunistic
nx9500-6C8809(config-profile-testAP7161-if-radiol)#
```

Related Commands

|                                 |                                                        |
|---------------------------------|--------------------------------------------------------|
| <a href="#">no</a> on page 1114 | Resets the rate selection mode to standard (monotonic) |
|---------------------------------|--------------------------------------------------------|

rf-mode

[interface-config-radio-instance](#) on page 1072

Configures the radio's RF mode of operation

This command sets the mode to either 2.4 GHz WLAN or 5.0 GHz WLAN support depending on the radio's intended client support. If you are currently licensed to use 4.9 GHz, configure the 4.9 GHz-WLAN option.

Set the mode to sensor if using the radio for rogue device detection. The radio cannot support rogue detection when one of the other radios is functioning as a WIPS sensor. To set a radio as a detector, disable sensor support on the other access point radios.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

Syntax

```
rf-mode [2.4GHz-wlan | 4.9GHz-wlan | 5GHz-wlan | bridge | scan-ahead | sensor]
```

Parameters

```
rf-mode [2.4GHz-wlan | 4.9GHz-wlan | 5GHz-wlan | bridge | scan-ahead | sensor]
```

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>rf-mode</b>     | Configures the radio's RF mode of operation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>2.4GHz-wlan</b> | Provides WLAN service in the 2.4 GHz bandwidth                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>4.9GHz-wlan</b> | Provides WLAN service in the 4.9 GHz bandwidth                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>5GHz-wlan</b>   | Provides WLAN service in the 5.0 GHz bandwidth                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>bridge</b>      | <p>Enables this radio to operate as client bridge that can authenticate and associate to a defined infrastructure Wireless LAN (WLAN) access point</p> <p><b>Note:</b> This option is applicable only on the AP6522, AP6562, AP7522, AP7532, and AP7562 model access points. Enable this option only if the access point is to provide client-bridge support. Once enabled, configure the client-bridge parameters. For more information, see <a href="#">bridge</a> on page 1088.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>scan-ahead</b>  | <p>Enables this radio to operate as a scan-ahead radio</p> <p>A radio functioning in the scan-ahead mode is used for forward scanning only. The radio does not support WLAN or mesh services.</p> <p>The scan ahead feature is used in Dynamic Frequency Selection (DFS) aware countries for infrastructure devices, static, and vehicular mounted modems (VMMs). It enables a secondary radio to scan ahead for an active channel for backhaul transmission, in the event of a radar trigger on the primary radio. The device then switches radios allowing transmission to continue. This is required in environments where handoff is required and DFS triggers are common.</p> <p>With a secondary radio dedicated for forward scanning, the primary radio, in case of radar hit, hands over the channel availability check (CAC) function to the secondary radio. This avoids a break in data communication, which would have resulted if the primary radio was to do CAC itself.</p> <p>The secondary radio periodically does a scan of the configured channel list, searching for the other available meshpoint roots. When configured on the root meshpoint, the scan-ahead feature also scans for cleaner channels.</p> |
| <b>sensor</b>      | Operates as a sensor radio. Configures this radio to function as a scanner, providing scanning services on both 2.4 GHz and 5.0 GHz bands. The radio does not provide WLAN services.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

#### Example

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#rf-mode sensor
```

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#show context
```

```
interface radiol
 rf-mode sensor
 placement outdoor
 mesh client
 off-channel-scan channel-list 2.4GHz 1
 guard-interval long
 aggregation ampdu tx-only
 aeroscout forward
 ekahau forward ip 172.16.10.1 port 3
 non-unicast tx-rate bss 1 dynamic-all
 --More--
```

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#
```

#### Related Commands

|                                         |                                                |
|-----------------------------------------|------------------------------------------------|
| <a href="#">no</a> on page 1114         | Resets the radio's RF mode of operation        |
| <a href="#">data-rates</a> on page 1099 | Configures the 802.11 data rates on this radio |

rifs

[interface-config-radio-instance](#) on page 1072

Configures Reduced Interframe Spacing (RIFS) parameters on this radio

This value determines whether interframe spacing is applied to access point transmitted or received packets, both, or none. Inter-frame spacing is the interval between two consecutive Ethernet frames that enable a brief recovery between packets and allow target devices to prepare for the reception of the next packet.

Supported in the following platforms:

- Access Points – AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

Syntax

```
rifs [none|rx-only|tx-only|tx-rx]
```

Parameters

```
rifs [none|rx-only|tx-only|tx-rx]
```

|                |                                                                                                                 |
|----------------|-----------------------------------------------------------------------------------------------------------------|
| <b>rifs</b>    | Configures RIFS parameters                                                                                      |
| <b>none</b>    | Disables support for RIFS. Consider setting the value to None for high-priority traffic to reduce packet delay. |
| <b>rx-only</b> | Supports RIFS possession only                                                                                   |
| <b>tx-only</b> | Supports RIFS transmission only                                                                                 |
| <b>tx-rx</b>   | Supports both RIFS transmission and possession (default setting)                                                |

Example

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#rifs tx-only
```

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#show context
```

```
interface radiol
 rf-mode sensor
 placement outdoor
 mesh client
 off-channel-scan channel-list 2.4GHz 1
 guard-interval long
 aggregation ampdu tx-only
 rifs tx-only
 aeroscout forward
 ekahau forward ip 172.16.10.1 port 3
 non-unicast tx-rate bss 1 dynamic-all
 non-unicast tx-rate bss 2 highest-basic
 non-unicast tx-rate bss 3 highest-basic
 non-unicast tx-rate bss 4 highest-basic
--More--
```

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#
```

Related Commands

|                                 |                                  |
|---------------------------------|----------------------------------|
| <a href="#">no</a> on page 1114 | Disables radio's RIFS parameters |
|---------------------------------|----------------------------------|

rts-threshold

[interface-config-radio-instance](#) on page 1072

Configures the Request to Send (RTS) threshold value on this radio

RTS is a transmitting station's signal that requests a Clear To Send (CTS) response from a receiving client. This RTS/CTS procedure clears the air where clients are contending for transmission time. Benefits include fewer data collisions and better communication with nodes that are hard to find (or hidden) because of other active nodes in the transmission path.

The RTS threshold controls RTS/CTS by initiating an RTS/CTS exchange for data frames larger than the threshold, and sends (without RTS/CTS) any data frames smaller than the threshold.

Consider the trade-offs when setting an appropriate RTS threshold for the WLAN's access point radios. A lower RTS threshold causes more frequent RTS/CTS exchanges. This consumes more bandwidth because of additional latency (RTS/CTS exchanges) before transmissions can commence. A disadvantage is the reduction in data-frame throughput. An advantage is quicker system recovery from electromagnetic interference and data collisions. Environments with more wireless traffic and contention for transmission make the best use of a lower RTS threshold.

A higher RTS threshold minimizes RTS/CTS exchanges, consuming less bandwidth for data transmissions. A disadvantage is less help to nodes that encounter interference and collisions. An advantage is faster data-frame throughput. Environments with less wireless traffic and contention for transmission make the best use of a higher RTS threshold.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

Syntax

```
rts-threshold <0-65536>
```

Parameters

```
rts-threshold <0-65536>
```

|                                                |                                                                                   |
|------------------------------------------------|-----------------------------------------------------------------------------------|
| <b>rts-threshold</b><br><b>&lt;0-65536&gt;</b> | Specify the RTS threshold value from 0 - 65536 bytes. The default is 65536 bytes. |
|------------------------------------------------|-----------------------------------------------------------------------------------|

Example

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radio1)#rts-threshold 100
```

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radio1)#show context
```

```
interface radio1
 rf-mode sensor
 placement outdoor
 mesh client
 rts-threshold 100
 off-channel-scan channel-list 2.4GHz 1
 guard-interval long
 aggregation ampdu tx-only
```

--More--

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

|                        |                                               |
|------------------------|-----------------------------------------------|
| <b>no</b> on page 1114 | Resets a radio's RTS threshold to its default |
|------------------------|-----------------------------------------------|

service

[interface-config-radio-instance](#) on page 1072

Enables dynamic control function. This dynamic function controls performance of the radio receiver's low noise amplifiers (LNAs).

When enabled, the control function, in the presence of very strong received signals, improves the receiver's performance on radio 1. Strong signals are caused if the distance between the WiFi client and the AP is within two (2) meters. When disabled, the control function is a useful debug tool in case the uplink throughput is less than expected and the AP-to-client separation is greater than two (2) meters. Disabling the control function does not affect the receive sensitivity of the radio.

Supported in the following platforms:

- Access Points — AP6522, AP6562

Syntax

```
service radio-lna [agc|ms]
```

Parameters

```
service radio-lna [agc|ms]
```

|                                   |                                                                                                                                                                                 |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>service radio-lna [agc ms]</b> | Enables dynamic control function                                                                                                                                                |
|                                   | <ul style="list-style-type: none"><li>• agc - Enables dynamic LNA control function. This is the default setting.</li><li>• ms - Disables dynamic LNA control function</li></ul> |

Example

```
nx9500-6C8809(config-profile-testAP6522-if-radiol)#service radio-lna ms
```

```
nx9500-6C8809(config-profile-testAP6522-if-radiol)#show context
 interface radiol
 service radio-lna ms
nx9500-6C8809(config-profile-testAP6522-if-radiol)#
```

Related Commands

|                                 |                                         |
|---------------------------------|-----------------------------------------|
| <a href="#">no</a> on page 1114 | Reverts radio-lna mode to default (agc) |
|---------------------------------|-----------------------------------------|

shutdown

[interface-config-radio-instance](#) on page 1072

Terminates or shuts down selected radio interface

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

Syntax

```
shutdown
```

Parameters

None

Example

```
nx9500-6C8809nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#shutdown
```

Related Commands

no on page 1114

Enables a disabled radio interface

## smart-rf

[interface-config-radio-instance](#) on page 1072

Overrides Smart RF channel width setting on this radio. When configured, the radio overrides the Smart RF selected channel setting and operates in the channel configured using this command.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

Syntax

```
smart-rf preferred-channel-width [20MHz | 40MHz | 80MHz]
```

Parameters

```
smart-rf preferred-channel-width [20MHz | 40MHz | 80MHz]
```

|                                                                   |                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>smart-rf preferred-channel-width [ 20MHz   40MHz   80MHz ]</b> | Configures the preferred channel width. The options are: <ul style="list-style-type: none"><li>• 20MHz – Sets 20 MHz as the preferred channel of operation</li><li>• 40MHz – Sets 40MHz as the preferred channel of operation</li><li>• 80MHz – Sets 80MHz as the preferred channel of operation (default setting)</li></ul> |
|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Example

```
nx9500-6C8809(config-profile-testAP7161-if-radio1)#smart-rf preferred-channel-width 40MHz
```

```
nx9500-6C8809(config-profile-testAP7161-if-radio1)#show context
interface radio1
 smart-rf preferred-channel-width 40MHz
 rate-selection opportunistic
nx9500-6C8809(config-profile-testAP7161-if-radio1)#
```

Related Commands

no on page 1114

Enables use of Smart RF selected channel of operation

## sniffer-redirect

[interface-config-radio-instance](#) on page 1072

Captures and redirects packets to an IP address running a packet capture/analysis tool

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

Syntax

```
sniffer-redirect [omnipeek|tzsp] <IP> channel [1 | 10 | 100 | 100w -----]
{snap <1-65535> (append descriptor)}
```

Parameters

```
sniffer-redirect [omnipeek|tzsp] <IP> channel [1 | 10 | 100 | 100w -----] {snap <1-65535>
(append descriptor)}
```



|                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>sniffer-redirect</b>          | Captures and redirects packets to an IP address running a packet capture/analysis tool                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>omnipeek</b>                  | Encapsulates captured packets in proprietary header (used with OmniPeek and plug-in)                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>tzsp</b>                      | Encapsulates captured packets in TZSP (used with WireShark and other tools)                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>&lt;IP&gt;</b>                | Specify the IP address of the device running the capture/analysis tool (the host to which captured off channel scan packets are redirected)                                                                                                                                                                                                                                                                                                                                           |
| <b>[1 10 100 100w<br/>-----]</b> | Specify the channel to capture packets <ul style="list-style-type: none"> <li>• 1 – Channel 1 in 20 MHz mode (default setting)</li> <li>• 10 – Channel 10 in 20 MHz mode</li> <li>• 100 – Channel 100 in 20 MHz mode</li> <li>• 100w – Channels 100w in 40 MHz mode (channels 100*,104)</li> </ul>                                                                                                                                                                                    |
| <b>snap &lt;1-65535&gt;</b>      | Optional. Allows truncating of large captured frames at a specified length (in bytes). This option is useful when capturing traffic with large frames. Use this option when only headers are needed for analysis, since it reduces the bandwidth needed for sniffing, and (for typical values) eliminates any fragmentation of the outer packet. <ul style="list-style-type: none"> <li>• &lt;1-65535&gt; – Specify the maximum truncated byte length of captured packets.</li> </ul> |
| <b>append descriptor</b>         | Optional – Enables appending of the radio's receive descriptor to the captured packet                                                                                                                                                                                                                                                                                                                                                                                                 |

#### Example

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radio1)#sniffer-redirect omnipeek
172.16.10.1 channel 1
```

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radio1)#show context
interface radio1
 rf-mode sensor
 placement outdoor
 mesh client
 rts-threshold 100
 off-channel-scan channel-list 2.4GHz 1
 guard-interval long
 aggregation ampdu tx-only
 rifs tx-only
 sniffer-redirect omnipeek 172.16.10.1 channel 1
 aeroscout forward
 ekahau forward ip 172.16.10.1 port 3
 non-unicast tx-rate bss 1 dynamic-all
 non-unicast tx-rate bss 2 highest-basic
 non-unicast tx-rate bss 3 highest-basic
 non-unicast tx-rate bss 4 highest-basic
 non-unicast tx-rate bss 5 highest-basic
 non-unicast tx-rate bss 6 highest-basic
 --More--
nx9500-6C8809(config-profile-7lxxTestProfile-if-radio1)#
```

#### Related Commands

|                                 |                                         |
|---------------------------------|-----------------------------------------|
| <a href="#">no</a> on page 1114 | Disables packet capture and redirection |
|---------------------------------|-----------------------------------------|

stbc

[interface-config-radio-instance](#) on page 1072

Configures the radio's Space Time Block Coding (STBC) mode. STBC is a pre-transmission encoding scheme providing an improved SNR ratio (even at a single RF receiver). STBC transmits multiple data stream copies across multiple antennas. The receiver combines the copies into one to retrieve data from the signal. These transmitted data versions provide redundancy to increase the odds of receiving data streams with a good data decode (especially in noisy environments).



#### Note

STBC requires the radio has at least two antennas with the capability to transmit two streams. If the antenna mode is configured to 1x1 (or falls back to 1x1 for some reason), STBC support is automatically disabled.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

Syntax

```
stbc [auto|none|tx-only]
```

Parameters

```
stbc [auto|none|tx-only]
```

|                |                                                                                                                       |
|----------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>stbc</b>    | Configures the radio's STBC mode                                                                                      |
| <b>auto</b>    | Autoselects STBC settings based on the platform type and other radio interface settings. This is the default setting. |
| <b>none</b>    | Disables STBC support                                                                                                 |
| <b>tx-only</b> | Configures the AP radio to format and broadcast the special stream (enables STBC support for transmit only)           |

Example

```
nx9500-6C8809(config-profile-81xxTestProfile-if-radio1)#stbc tx-only

rfs6000-37FABE(config-profile-81xxTestProfile-if-radio1)#show context
interface radio1
stbc tx-only
nx9500-6C8809(config-profile-81xxTestProfile-if-radio1)#
```

Related Commands

|                                 |                       |
|---------------------------------|-----------------------|
| <a href="#">no</a> on page 1114 | Disables STBC support |
|---------------------------------|-----------------------|

transmit-beamforming

[interface-config-radio-instance](#) on page 1072

Enables transmit beamforming on this radio interface. This option is disabled by default.

When enabled, this option steers signals to peers in a specific direction to enhance signal strength and improve throughput amongst meshed devices (not clients). Each access point radio supports up to 16 beamforming capable mesh peers. When enabled, a beamformer steers its wireless signals to its peers. A beamformee device assists the beamformer with channel estimation by providing a feedback matrix. The feedback matrix is a set of values sent by the beamformee to assist the beamformer in computing a steering matrix. A steering matrix is an additional set of values used to steer wireless signals at the beamformer so constructive signals arrive at the beamformee for better SNR and throughput. Any

beamforming capable mesh peer connecting to a radio whose capacity is exhausted cannot enable beamforming itself.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP8122, AP8132, AP8163, AP8432, AP8533

Syntax

**transmit-beamforming**

Parameters

None

Example

```
nx9500-6c8809(config-profile-testAP8163-if-radio1)#transmit-beamforming
```

Related Commands

|                                 |                                                       |
|---------------------------------|-------------------------------------------------------|
| <a href="#">no</a> on page 1114 | Disables transmit beamforming on this radio interface |
|---------------------------------|-------------------------------------------------------|

use

[interface-config-radio-instance](#) on page 1072

Applies an association ACL policy and a radio QoS policy on this radio interface

An association ACL is a policy-based Access Control List (ACL) that either prevents or allows wireless clients from connecting to a controller managed access point radio. An ACL is a sequential collection of permit and deny conditions that apply to controller packets. When a packet is received on an interface, the controller compares the fields in the packet against any applied ACLs to verify the packet has the required permissions to be forwarded, based on the criteria specified in the access lists. If a packet does not meet any of the criteria specified in the ACL, the packet is dropped.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

Syntax

```
use [association-acl-policy|radio-qos-policy]
```

```
use [association-acl-policy <ASSOC-ACL-POLICY-NAME>|radio-qos-policy <RADIO-QOS-POLICY-NAME>]
```

Parameters

```
use [association-acl-policy <ASSOC-ACL-POLICY-NAME>|radio-qos-policy <RADIO-QOS-POLICY-NAME>]
```

|                               |                                                                                                                                                                                                                                        |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>use</b>                    | Applies an association ACL policy and a radio QoS policy on this radio interface                                                                                                                                                       |
| <b>association-acl-policy</b> | Uses a specified association ACL policy with this radio interface <ul style="list-style-type: none"><li>• &lt;ASSOC-ACL-POLICY-NAME&gt; - Specify the association ACL policy name (should be existing and fully configured).</li></ul> |
| <b>radio-qos-policy</b>       | Uses a specified radio QoS policy with this radio interface <ul style="list-style-type: none"><li>• &lt;RADIO-QoS-POLICY-NAME&gt; - Specify the radio QoS policy name (should be existing and fully configured).</li></ul>             |

## Example

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#use association-acl-policy test

nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#show context
interface radiol
 rf-mode sensor
 placement outdoor
 mesh client
 rts-threshold 100
 off-channel-scan channel-list 2.4GHz 1
 guard-interval long
 aggregation ampdu tx-only
 rifs tx-only
 use association-acl-policy test
 sniffer-redirect omnipeek 172.16.10.1 channel 1
 aeroscout forward
 ekahau forward ip 172.16.10.1 port 3
 --More--
nx9500-6C8809(config-profile-71xxTestProfile-if-radiol)#
```

## Related Commands

|                                 |                                                                       |
|---------------------------------|-----------------------------------------------------------------------|
| <a href="#">no</a> on page 1114 | Dissociates the specified association ACL policy and radio QoS policy |
|---------------------------------|-----------------------------------------------------------------------|

## wips

[interface-config-radio-instance](#) on page 1072

Enables access point to change its channel of operation in order to terminate rogue devices. The radio should be configured to provide WLAN service.

This option is enabled by default.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533



### Note

AP7522 and AP7532 access points use Smart RF to perform off-channel scans. Therefore, ensure that a Smart RF policy is configured and applied to AP7522 and AP7532 access points RF Domains to enable them perform rogue detection and termination.

## Syntax

```
wips airtime-termination allow-channel-change
```

## Parameters

```
wips airtime-termination allow-channel-change
```

|                                                      |                                                                                                                              |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>wips airtime-termination allow-channel-change</b> | Enables access point to change its channel of operation (to that of the rogue device) in order to terminate the rogue device |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|

## Example

```
nx9500-6C8809(config-profile-testAP8163-if-radiol)#wips air-termination allow-channel-change
```

## Related Commands

no on page 1114

Disables access point to change its channel of operation in order to terminate rogue devices

wireless-client

[interface-config-radio-instance](#) on page 1072

Configures wireless client parameters on this radio

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

Syntax

```
wireless-client tx-power [<0-20>|mode]
```

```
wireless-client <0-20>
```

```
wireless-client tx-power mode [802.11d {wing-ie}/wing-ie {802.11d}]
```

Parameters

```
wireless-client tx-power <0-20>
```

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>wireless-client</b>       | Configures wireless client parameters                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>tx-power &lt;0-20&gt;</b> | Configures the transmit power indicated to wireless clients. If using a dual or three radio model access point, each radio should be configured with a unique transmit power in respect to its intended client support function. A setting of 0 defines the radio as using Smart RF to determine its output power. 20 dBm is the default value. <ul style="list-style-type: none"><li>• &lt;0-20&gt; - Specify transmit power from 0 - 20 dBm.</li></ul> |

```
wireless-client tx-power mode [802.11d {wing-ie}|wing-ie {802.11d}]
```

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>wireless-client</b>            | Configures wireless client parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>tx-power [802.11d wing-ie]</b> | Configures the transmit power indicated to wireless clients <ul style="list-style-type: none"><li>• 802.11d - Advertises in the IEEE 802.11d country information element<ul style="list-style-type: none"><li>• wing-ie - Optional. Advertises in the WiNG information element (173)</li></ul></li><li>• wing-ie - Advertises in the WiNG information element (173). This is the default setting.<ul style="list-style-type: none"><li>• 802.11d - Optional. Advertises in the IEEE 802.11d country information element</li></ul></li></ul> |

Example

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#wireless-client tx-power 20
```

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radiol)#show context
interface radiol
 rf-mode sensor
 placement outdoor
 mesh client
 rts-threshold 100
 wireless-client tx-power 20
 off-channel-scan channel-list 2.4GHz 1
 guard-interval long
 aggregation ampdu tx-only
```

--More--  
nx9500-6C8809(config-profile-7lxxTestProfile-if-radio1)#

#### Related Commands

|                 |                                                         |
|-----------------|---------------------------------------------------------|
| no on page 1114 | Resets the transmit power indicated to wireless clients |
|-----------------|---------------------------------------------------------|

wlan

[interface-config-radio-instance](#) on page 1072

Enables a WLAN on this radio

Use this command to configure WLAN/BSS mappings for an existing access point deployment. Administrators can assign each WLAN its own BSSID. If using a single-radio access point, there are 8 BSSIDs available. If using a dual-radio access point there are 8 BSSIDs for the 802.11b/g/n radio and 8 BSSIDs for the 802.11a/n radio.

Supported in the following platforms:

- Access Points – AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

#### Syntax

```
wlan <WLAN-NAME> {bss/primary}
```

```
wlan <WLAN-NAME> {bss <1-16>} {primary}
```

#### Parameters

```
wlan <WLAN-NAME> {bss <1-16>} {primary}
```

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;WLAN-NAME&gt; {bss</b> | Specify the WLAN name (it must have been already created and configured)                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>&lt;1-16&gt;  primary}</b> | <ul style="list-style-type: none"><li>• bss &lt;1-16&gt; - Optional. Specifies a BSS for the radio to map the WLAN<ul style="list-style-type: none"><li>• &lt;1-18&gt; - Specify the BSS number from 1 - 16.</li></ul></li><li>• primary - Optional. Uses the specified WLAN as the primary WLAN, when multiple WLANs exist on the BSS</li><li>• primary - Optional. Uses the specified WLAN as the primary WLAN, when multiple WLANs exist on the BSS</li></ul> |

#### Example

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radio1)#wlan TestWLAN primary
```

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radio1)#show context
```

```
interface radio1
 rf-mode sensor
 placement outdoor
 mesh client
 rts-threshold 100
 wireless-client tx-power 20
 wlan TestWLAN bss 1 primary
 off-channel-scan channel-list 2.4GHz 1
 guard-interval long
 aggregation ampdu tx-only
 rifs tx-only
 use association-acl-policy test
 sniffer-redirect omnipeek 172.16.10.1 channel 1
 aeroscout forward
 ekahau forward ip 172.16.10.1 port 3
```

```
non-unicast tx-rate bss 1 dynamic-all
non-unicast tx-rate bss 2 highest-basic
```

--More--

```
nx9500-6C8809(config-profile-7lxxTestProfile-if-radio1)#
```

#### Related Commands

|                                 |                            |
|---------------------------------|----------------------------|
| <a href="#">no</a> on page 1114 | Disables a WLAN on a radio |
|---------------------------------|----------------------------|

## interface-config-wwan-instance

[interface](#) on page 1013

A Wireless Wide Area Network (WWAN) card is a specialized network interface card that allows a device to connect, transmit and receive data over a Cellular Wide Area Network. The RFS4000 and RFS6000 each have a PCI Express card slot that supports 3G WWAN cards. The WWAN card uses point to point protocol (PPP) to connect to the Internet Service Provider (ISP) and gain access to the Internet. PPP is the protocol used for establishing Internet links over dial-up modems, DSL connections, and many other types of point-to-point communications. PPP packages your system's TCP/IP packets and forwards them to the serial device where they can be put on the network. PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

To switch to the WWAN Interface configuration mode, use the following command:

```
<DEVICE>(config)#profile <DEVICE-TYPE> <DEVICE-PROFILE-NAME>
```

```
<DEVICE>(config-profile-<DEVICE-PROFILE-NAME>)#interface wwan1
```

```
<DEVICE>(config-profile-<DEVICE-PROFILE-NAME>)#?
```

Interface configuration commands:

|             |                                                              |
|-------------|--------------------------------------------------------------|
| apn         | Enter the access point name provided by the service provider |
| auth-type   | Type of authentication, Eg chap, pap                         |
| crypto      | Encryption Module                                            |
| description | Port description                                             |
| ip          | Internet Protocol (IP)                                       |
| no          | Negate a command or set its defaults                         |
| password    | Enter password provided by the service provider              |
| shutdown    | Disable wireless wan feature                                 |
| use         | Set setting to use                                           |
| username    | Enter username provided by the service provider              |

|         |                                                   |
|---------|---------------------------------------------------|
| clrscr  | Clears the display screen                         |
| commit  | Commit all changes made in this session           |
| do      | Run commands from Exec mode                       |
| end     | End current mode and change to EXEC mode          |
| exit    | End current mode and down to previous mode        |
| help    | Description of the interactive help system        |
| revert  | Revert changes                                    |
| service | Service Commands                                  |
| show    | Show running system information                   |
| write   | Write running configuration to memory or terminal |

```
<DEVICE>(config-profile-<DEVICE-PROFILE-NAME>)#
```

The following table summarizes WWAN interface configuration commands:

| Commands                               | Description                                                         |
|----------------------------------------|---------------------------------------------------------------------|
| <a href="#">apn</a> on page 1140       | Configures the access point's name provided by the service provider |
| <a href="#">auth-type</a> on page 1140 | Configures the authentication types used on this interface          |
| <a href="#">crypto</a> on page 1141    | Associates a crypto map with this interface                         |
| <a href="#">ip</a> on page 1142        | Associates an IP ACL with this interface                            |
| <a href="#">no</a> on page 1143        | Removes or reverts the WWAN interface settings                      |
| <a href="#">password</a> on page 1144  | Configures a password for this WWAN interface                       |
| <a href="#">use</a> on page 1145       | Associates an IP ACL with this interface                            |
| <a href="#">username</a> on page 1146  | Configures the names of users accessing this interface              |

apn

[interface-config-wwan-instance](#) on page 1139

Configures the cellular data provider's name. This setting is needed in areas with multiple cellular data providers using the same protocols, such as Europe and Asia.

Supported in the following platforms:

- Access Point — AP7161, AP8163
- Wireless Controllers — RFS4000

Syntax

**apn** <WORD>

Parameters

apn <WORD>

|                   |                                                         |
|-------------------|---------------------------------------------------------|
| <b>apn</b> <WORD> | Specify the name of the cellular data service provider. |
|-------------------|---------------------------------------------------------|

Example

```
nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#apn AT&T

nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#show context
 interface wwan1
 apn AT&T
nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#
```

Related Commands

|                                 |                                           |
|---------------------------------|-------------------------------------------|
| <a href="#">no</a> on page 1143 | Removes the configured access point name. |
|---------------------------------|-------------------------------------------|

auth-type

[interface-config-wwan-instance](#) on page 1139

Configures the authentication type used by the cellular data provider

Supported in the following platforms:



- Access Point — AP7161, AP8163
- Wireless Controllers — RFS4000

#### Syntax

```
auth-type [chap | mschap | mschap-v2 | pap]
```

#### Parameters

```
auth-type [chap | mschap | mschap-v2 | pap]
```

|                  |                                                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------|
| <b>auth-type</b> | Configures the authentication protocol used on this interface. The options are: PAP, CHAP, MSCHAP, and MSCHAP-v2 |
| <b>chap</b>      | Configures Challenge-Handshake Authentication Protocol (CHAP). This is the default value.                        |
| <b>mschap</b>    | Configures Microsoft Challenge-Handshake Authentication Protocol (MSCHAP)                                        |
| <b>mschapv2</b>  | Configures Microsoft Challenge-Handshake Authentication Protocol (MSCHAP) version 2                              |
| <b>pap</b>       | Configures Password Authentication Protocol (PAP)                                                                |

#### Example

```
nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#auth-type mschap-v2

nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#show context
interface wwan1
 apn AT&T
 auth-type mschap-v2
nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#
```

#### Related Commands

|                                 |                                                                  |
|---------------------------------|------------------------------------------------------------------|
| <a href="#">no</a> on page 1143 | Removes the authentication protocol configured on this interface |
|---------------------------------|------------------------------------------------------------------|

## crypto

[interface-config-wwan-instance](#) on page 1139

Associates a crypto map with this interface

Supported in the following platforms:

- Access Point — AP7161, AP8163
- Wireless Controllers — RFS4000

#### Syntax

```
crypto map <CRYPTO-MAP-NAME>
```

#### Parameters

```
crypto map <CRYPTO-MAP-NAME>
```

|                                                     |                                                                                                                                                                                            |
|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>crypto map</b><br><b>&lt;CRYPTO-MAP-NAME&gt;</b> | Associates a crypto map with this interface <ul style="list-style-type: none"> <li>• &lt;CRYPTO-MAP-NAME&gt; - Specify the crypto map name (should be existing and configured).</li> </ul> |
|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Example

```
nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#crypto map test

nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#show context
```

```

interface wwan1
 apn AT&T
 auth-type mschap-v2
 crypto map test
nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#

```

#### Related Commands

|                                 |                                                       |
|---------------------------------|-------------------------------------------------------|
| <a href="#">no</a> on page 1143 | Removes the crypto map associated with this interface |
|---------------------------------|-------------------------------------------------------|

ip

[interface-config-wwan-instance](#) on page 1139

Configures IP related settings on this interface

Supported in the following platforms:

- Access Point – AP7161, AP8163
- Wireless Controllers – RFS4000

Syntax

```
ip [default-gateway|nat]
```

```
ip default-gateway priority <1-8000>
```

```
ip nat [inside|outside]
```

Parameters

```
ip default-gateway priority <1-8000>
```

|                                                |                                                                                                                                                                                                   |
|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ip</b>                                      | Configures IP related settings on this interface                                                                                                                                                  |
| <b>default-gateway priority &lt;1-8000&gt;</b> | Configures the default-gateway's (learned by the wireless WAN) priority. <ul style="list-style-type: none"> <li>• &lt;1-8000&gt; – Specify a value from 1 - 8000. The default is 3000.</li> </ul> |

```
ip nat [inside|outside]
```

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ip</b>                   | Configures IP related settings on this interface                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>nat [inside outside]</b> | Configures the NAT settings. This option is disabled by default. <ul style="list-style-type: none"> <li>• inside – Marks this WWAN interface as NAT inside. The inside network is transmitting data over the network to its intended destination. On the way out, the source IP address is changed in the header and replaced by the (public) IP address.</li> <li>• outside – Marks this WWAN interface as NAT outside. Packets passing through the NAT on the way back to the controller or service platform managed LAN are matched against the records kept by the NAT engine. There, the destination IP address is changed back to the specific internal private class IP address in order to reach the LAN over the network.</li> </ul> |

Example

```
nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#ip default-gateway priority 1
```

```
nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#ip nat inside
```

```
nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#show context
```

```

interface wwan1
 apn AT&T
 auth-type mschap-v2
 crypto map test
 ip nat inside
 ip default-gateway priority 1
nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#

```

#### Related Commands

|                              |                                               |
|------------------------------|-----------------------------------------------|
| <code>no</code> on page 1143 | Removes IP related settings on this interface |
|------------------------------|-----------------------------------------------|

no

[interface-config-wwan-instance](#) on page 1139

Removes or reverts the WWAN interface settings

Supported in the following platforms:

- Access Point — AP7161, AP8163
- Wireless Controllers — RFS4000

#### Syntax

```
no [all | apn | auth-type | crypto | description | ip | password | shutdown | use |
username]
```

```
no [all | apn | auth-type | description | password | shutdown | username]
```

```
no crypto map
```

```
no ip [default-gateway priority | nat]
```

```
no use ip-access-list in
```

#### Parameters

```
no <PARAMETERS>
```

|                                        |                                                                                  |
|----------------------------------------|----------------------------------------------------------------------------------|
| <b>no</b><br><b>&lt;PARAMETERS&gt;</b> | Removes or reverts this WWAN interface's settings based on the parameters passed |
|----------------------------------------|----------------------------------------------------------------------------------|

#### Usage Guidelines

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

#### Example

The following example displays the WWAN interface settings before the 'no' commands are executed:

```

nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#show context
interface wwan1
 apn AT&T
 auth-type mschap-v2
 crypto map test
 ip nat inside
 ip default-gateway priority 1
nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#

```



```
nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#no apn
nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#no auth-type
```

The following example displays the WWAN interface settings after the 'no' commands are executed:

```
nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#show context
interface wwan1
 crypto map test
 ip nat inside
 ip default-gateway priority 1
nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#
password
```

[interface-config-wwan-instance](#) on page 1139

Configures a password for this WWAN interface. The configured value is used for authentication support by the cellular data carrier.

Supported in the following platforms:

- Access Point — AP7161, AP8163
- Wireless Controllers — RFS4000

Syntax

```
password [2 <WORD> | <WORD>]
```

Parameters

```
password [2 <WORD> | <WORD>]
```

|                       |                                                                                                       |
|-----------------------|-------------------------------------------------------------------------------------------------------|
| <b>password</b>       | Configures a password for this WWAN interface                                                         |
| <b>2 &lt;WORD&gt;</b> | Configures an encrypted password. Use this option when copy pasting the password from another device. |
| <b>&lt;WORD&gt;</b>   | Enter the password string (should not exceed 32 characters in length).                                |

Example

```
nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#password 2 TechPubsTesting@123

nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#show context
interface wwan1
 password TechPubsTesting@123
 crypto map test
 ip nat inside
 ip default-gateway priority 1
nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#
```

Related Commands

|                        |                                 |
|------------------------|---------------------------------|
| <b>no</b> on page 1143 | Removes the configured password |
|------------------------|---------------------------------|

shutdown

[interface-config-wwan-instance](#) on page 1139

Shuts down this WWAN interface. Use the no > shutdown command to re-start the WWAN interface.

Supported in the following platforms:

- Access Point — AP7161, AP8163
- Wireless Controllers — RFS4000

## Syntax

**shutdown**

## Parameters

None

## Example

```
nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#shutdown

nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#show context
 interface wwan1
 shutdown
nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#
```

## Related Commands

|                                 |                              |
|---------------------------------|------------------------------|
| <a href="#">no</a> on page 1143 | Re-starts the WWAN interface |
|---------------------------------|------------------------------|

use

[interface-config-wwan-instance](#) on page 1139

Associates an IP ACL with this interface. The ACL should be existing and configured.

The ACL applies an IP based firewall to all incoming packets. The ACL identifies a single IP or a range of IPs that are to be allowed or denied access on this interface.

Supported in the following platforms:

- Access Point — AP7161, AP8163
- Wireless Controllers — RFS4000

## Syntax

**use ip-access-list in <ACCESS-LIST-NAME>**

## Parameters

**use ip-access-list in <ACCESS-LIST-NAME>**

|                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>use ip-access-list in &lt;ACCESS-LIST-NAME&gt;</b> | Associates an inbound IPv4 ACL with this interface. This setting applies to IPv4 inbound traffic only and not IPv6 traffic. IPv4 operates as a best effort delivery method, as it does not guarantee delivery, and does not ensure proper sequencing or duplicate delivery (unlike TCP). IPv4 hosts can use link local addressing to provide local connectivity. <ul style="list-style-type: none"><li>• &lt;ACCESS-LIST-NAME&gt; - Specify the IP ACL name.</li></ul> |
|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Example

```
nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#use ip-access-list in test

nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#show context
 interface wwan1
 password TechPubsTesting@123
 crypto map test
 ip nat inside
 use ip-access-list in test
 ip default-gateway priority 1
nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#
```

## Related Commands

---

`no` on page 1143      Removes the IP ACL associated with this interface

username

[interface-config-wwan-instance](#) on page 1139

Configures the names of users accessing this interface

Supported in the following platforms:

- Access Point — AP7161, AP8163
- Wireless Controllers — RFS4000

Syntax

`username <WORD>`

Parameters

`username <WORD>`

|                                        |                                                                                                                                                                                                                       |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>username</b><br><b>&lt;WORD&gt;</b> | Configures the username for authentication support by the cellular data carrier <ul style="list-style-type: none"><li>• <code>&lt;WORD&gt;</code> - Specify the username (should not exceed 32 characters).</li></ul> |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Example

```
nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#username TechPubsUser1
```

```
nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#show context
interface wwan1
 username TechPubsUser1
 password TechPubsTesting@123
 crypto map test
 ip nat inside
 use ip-access-list in test
 ip default-gateway priority 1
nx9500-6C8809(config-profile-testRFS4000-if-wwan1)#
```

Related Commands

|                              |                                 |
|------------------------------|---------------------------------|
| <code>no</code> on page 1143 | Removes the configured username |
|------------------------------|---------------------------------|

## interface-config-bluetooth-instance

[interface](#) on page 1013

AP8432 and AP8533 model access points utilize a built-in Bluetooth chip for specific Bluetooth functional behaviors in a WiNG managed network. AP8432 and AP8533 models support both Bluetooth classic and Bluetooth low energy (BLE) technology. These platforms use their Bluetooth classic enabled radio to sense other Bluetooth enabled devices and report device data (MAC address, RSSI and device calls) to an ADSP server for intrusion detection. If the device presence varies in an unexpected manner, ADSP can raise an alarm.



### Note

AP8132 model access points support an external USB Bluetooth radio providing ADSP Bluetooth classic sensing functionality only, not the BLE beaconing functionality available for AP8432 and AP8533 model access points described in this section.

AP8432 and AP8533 model access points support Bluetooth beaconing to emit either iBeacon or Eddystone-URL beacons. The access point's Bluetooth radio sends non-connectable, undirected low-energy (LE) advertisement packets periodically. These advertisement packets are short and sent on Bluetooth advertising channels that conform to already-established iBeacon and Eddystone-URL standards. However, portions of the advertising packet are customizable via the Bluetooth radio interface configuration context.

To switch to this mode, use the following commands:

```
<DEVICE>(config)#profile <ap8432/ap8533> <PROFILE-NAME>

<DEVICE>(config-profile-default-ap8432)#interface bluetooth ?
 <1-1> Bluetooth interface index?
```

The following example uses the default-ap8432 profile instance to configure the Bluetooth radio interface:

```
nx9500-6C8809(config-profile-default-ap8432)#interface bluetooth 1
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)# Bluetooth Radio Mode commands:
 beacon Configure low-energy beacon operation parameters
 description Configure a description for this bluetooth radio
 eddystone Configure eddystone beacon payload parameters
 ibeacon Configure iBeacon beacon payload parameters
 mode Set the bluetooth operation mode
 no Negate a command or set its defaults
 shutdown Shutdown the selected bluetooth radio interface

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#
```

| Commands                                 | Description                                                                                                                                                                                                  |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">beacon</a> on page 1147      | Configures the Bluetooth radio's beacon's emitted transmission pattern                                                                                                                                       |
| <a href="#">description</a> on page 1149 | Configures a description for the Bluetooth radio interface                                                                                                                                                   |
| <a href="#">eddystone</a> on page 1150   | Configures Eddystone beacon payload parameters. Configure these parameters if the operational mode is set to 'le-beacon' and the beacon transmission pattern is set to 'eddystone-url1' or 'eddystone-url2'. |
| <a href="#">ibeacon</a> on page 1151     | Configures iBeacon beacon payload parameters. Configure these parameters if the operational mode is set to 'le-beacon' and the beacon transmission pattern is set to 'ibeacon'.                              |
| <a href="#">mode</a> on page 1152        | Configures the Bluetooth radio's mode of operation                                                                                                                                                           |
| <a href="#">shutdown</a> on page 1153    | Shut downs the selected Bluetooth radio interface                                                                                                                                                            |
| <a href="#">no</a> on page 1153          | Removes or reverts to default this Bluetooth radio interface's settings                                                                                                                                      |

beacon

[interface-config-bluetooth-instance](#) on page 1146

Configures the Bluetooth radio's beacon's emitted transmission pattern for Bluetooth radios functioning in the low energy beacon (le-beacon) mode. This option is applicable only if the Bluetooth radio's operational mode is set to le-beacon.

Supported in the following platforms:

- Access Points - AP8432, AP8533

Syntax

```
beacon [pattern|period|txpower]
```

```
beacon pattern [eddytone-url1|eddytone-ulr2|ibeacon]
```

```
beacon period <100-10000>
```

```
beacon txpower <-15-6>
```

Parameters

```
beacon pattern [eddytone-url1|eddytone-ulr2|ibeacon]
```

|                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>beacon pattern</b><br><b>[eddytone-<br/>url1  <br/>eddytone-<br/>ulr2   ibeacon]</b> | <p>When the beacon mode is set to 'le-beacon', use this command to configure the Bluetooth radio's beacon's emitted transmission pattern. Select one of the following beacon patterns:</p> <ul style="list-style-type: none"><li>• eddytone-url1 - Transmits an Eddystone-URL beacon using URL 1. This is the default setting.</li><li>• eddytone-ulr2 - Transmits an Eddystone-URL beacon using URL 2</li></ul> <p>An Eddystone-URL frame broadcasts a URL using a compressed encoding scheme to better fit within a limited advertisement packet. Once decoded, the URL can be used by a client for Internet access. If an Eddystone-URL beacon broadcasts https:anysite, clients receiving the packet can access that URL. If setting the transmission pattern as 'eddytone-url1' or 'eddytone-ulr2', use the 'eddytone' keyword to configure Eddystone beacon payload parameters. For more information, see <a href="#">eddytone</a> on page 1150.</p> <ul style="list-style-type: none"><li>• ibeacon - Transmits an ibeacon beacon. iBeacon was created by Apple for use in iPhone OS (iOS) devices (beginning with iOS version 7.0). There are three data fields Apple has made available to iOS applications, a Universally Unique Identifier (UUID) for device identification, a Major value for device class and a Minor value for more refined information like product category. If setting the transmission pattern as 'ibeacon', use the 'ibeacon' keyword to configure ibeacon beacon payload parameters. For more information, see <a href="#">ibeacon</a> on page 1151.</li></ul> <p>For more information on configuring the Bluetooth radio's operational mode, see <a href="#">mode</a> on page 1152.</p> |
|-----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
beacon period <100-10000>
```

|                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>beacon period</b><br><b>&lt;100-10000&gt;</b> | <p>Configures the Bluetooth radio's beacon transmission period, in milliseconds, from 100 - 10000. As the defined period increases, so does the CPU processing time and the number of packets incrementally transmitted (typically one per minute).</p> <ul style="list-style-type: none"><li>• &lt;100-10000&gt; - Specify a value from 100 - 10000 milliseconds. The default value is 1000 milliseconds.</li></ul> |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
beacon txpower <-15-6>
```



```
beacon txpower <-15-6>
```

Configures the Bluetooth radio's le-beacon transmit power. This determines how far a beacon can transmit data.

- <-15-6> - Specify a value from -15 - -6 dBm. The default value is -10 dBm.

#### Example

```
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#beacon pattern eddystone-url2
```

```
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#beacon period 900
```

```
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#show context
interface bluetooth1
 shutdown
 description AP8432-BLE-Radiol
 mode le-beacon
 beacon pattern eddystone-url2
 beacon period 900
```

```
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#
```

#### Related Commands

[no](#) on page 1153

Removes or reverts to default this Bluetooth radio's beacon-related configurations

#### description

[interface-config-bluetooth-instance](#) on page 1146

Configures a description for the Bluetooth radio interface, differentiating it from other Bluetooth supported radio's within the same RF Domain

Supported in the following platforms:

- Access Points - AP7602, AP7612, AP7622, AP7632, AP7662, AP8432, AP8533

#### Syntax

```
description <WORD>
```

#### Parameters

```
description <WORD>
```

**description**  
**<WORD>**

Configures a description for the AP8432/AP8533 access point's Bluetooth radio's description

- <WORD> - Provide a description that uniquely identifies this radio interface from other similar Bluetooth supported radios (should not exceed 64 characters) within an RF Domain.

#### Example

```
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#description AP8432-BLE-Radiol
```

```
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#show context
interface bluetooth1
 shutdown
 description AP8432-BLE-Radiol
```

```
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#
```

#### Related Commands

no on page 1153

Removes this Bluetooth radio interface's description

eddystone

[interface-config-bluetooth-instance](#) on page 1146

Configures Eddystone beacon payload parameters. Configure these parameters only if the Bluetooth radio interface's operational mode is set to 'le-beacon', and the beacon's emitted transmission pattern is set to either 'eddystone-url1' or 'eddystone-url2'.

Supported in the following platforms:

- Access Points - AP7602, AP7612, AP7622, AP7632, AP7662, AP8432, AP8533

Syntax

```
eddystone [calibration-rssi <-127-127>|url [1|2] <WORD>]
```

Parameters

```
eddystone [calibration-rssi|url [1|2] <WORD>]
```

```
eddystone
[calibration-
rss
<-127-127>|
url [1|2]
<WORD>]
```

If the Beacon transmission pattern has been set to either 'eddystone-url1' or 'eddystone-url2', configure the following Eddystone parameters:

- calibration-rssi - Configures the Eddystone beacon measured calibration signal strength, from -127 to 127 dBm, at 0 meters. Mobile devices can approximate their distance to beacons based on received signal strength. However, distance readings can fluctuate since they depend on several external factors. The closer you are to a beacon, the more accurate the reported distance. This setting is the projected calibration signal strength at 0 meters.
  - <-127-127> - Specify a value from -127 - 127 dBm. The default value is -19 dBm.
- url [1|2] <WORD> - Configures the Eddystone URL as URL1 OR URL2
  - 1 - Selects the Eddystone URL number 1
  - 2 - Selects the Eddystone URL number 2

The following keyword is common to the 'eddystone-url1' and 'eddystone-url2' keywords:

- <WORD> - Enter a 64 character maximum eddystone-URL1/eddystone-URL2. The URL must be 18 characters or less once auto-encoding is applied. URL encoding is used when placing text in a query string to avoid confusion with the URL itself. It is typically used when a browser sends data to a Web server.

Example

```
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#eddystone calibration-rssi -120
```

```
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#show context
interface bluetooth1
shutdown
description AP8432-BLE-Radiol
mode le-beacon
beacon pattern eddystone-url2
beacon period 900
eddystone calibration-rssi -120
```

```
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#
```

Related Commands

- [no](#) on page 1153

Removes or reverts to default this Bluetooth radio's Eddystone beacon payload configurations

## ibeacon

[interface-config-bluetooth-instance](#) on page 1146

Configures iBeacon beacon payload parameters. Configure these parameters only if the Bluetooth radio interface's operational mode is set to 'le-beacon', and the beacon's emitted transmission pattern is set to 'ibeacon'.

Supported in the following platforms:

- Access Points - AP7602, AP7612, AP7622, AP7632, AP7662, AP8432, AP8533

Syntax

```
ibeacon [calibration-rssi <-127-127>|major <0-65535>|minor <0-65535>|uuid <WORD>]
```

```
ibeacon [calibration-rssi <-127-127>|uuid <WORD>]
```

```
ibeacon [major|minor] <0-65535>
```

Parameters

```
ibeacon [calibration-rssi <-127-127>|major <0-65535>|minor <0-65535>|uuid <WORD>]
```

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ibeacon</b>                           | Configures following iBeacon beacon payload parameters: calibration-rssi, major, minor, and uuid                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>calibration-rssi &lt;-127-127&gt;</b> | Configures the iBeacon measured calibration signal strength, from -127 to 127 dBm, at 1 meter. Mobile devices can approximate their distance to beacons based on received signal strength. However, distance readings can fluctuate since they depend on several external factors. The closer you are to a beacon, the more accurate the reported distance. This setting is the projected calibration signal strength at 1 meter. <ul style="list-style-type: none"><li>• &lt;-127-127&gt; - Specify a value from -127 - 127 dBm. The default value is -60 dBm.</li></ul> |
| <b>major &lt;0-65535&gt;</b>             | Configures the iBeacon Major value from 0 - 65535. Major values identify and distinguish groups. For example, each beacon on a specific floor in a building could be assigned a unique major value. <ul style="list-style-type: none"><li>• &lt;0-65535&gt; - Specify a value from 0 - 65535. The default value is 1111.</li></ul>                                                                                                                                                                                                                                        |
| <b>minor &lt;0-65535&gt;</b>             | Configures the iBeacon Minor value from 0 - 65535. Minor values identify and distinguish individual beacons. Minor values help identify individual beacons within a group of beacons assigned a major value. The default setting is 2,222. <ul style="list-style-type: none"><li>• &lt;0-65535&gt; - Specify a value from 0 - 65535. The default value is 2222.</li></ul>                                                                                                                                                                                                 |
| <b>uuid &lt;WORD&gt;</b>                 | Configures a 32 hex character maximum UUID. The UUID classification contains 32 hexadecimal digits, split into 5 groups, separated by dashes. For example, f2468da65fa82e841134bc5b71e0893e. The UUID distinguishes iBeacons in the network from all other beacons in networks outside of your direct administration. <ul style="list-style-type: none"><li>• &lt;WORD&gt; - Specify the UUID (should not exceed 32 hexadecimal characters). The default value is 01F101F101F101F101F101F101F101F1.</li></ul>                                                             |

Example

```
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#ibeacon calibration-rssi -70
```

```
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#ibeacon major 1110
```

```
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#ibeacon
```

```

minor 2210

nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#ibeacon uuid
f2468da65fa82e841134bc5b71e0893e

nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#show context
interface bluetooth1
 shutdown
 mode le-beacon
 beacon pattern ibeacon
 ibeacon calibration-rssi -70
 ibeacon major 1110
 ibeacon minor 2210
 ibeacon uuid f2468da65fa82e841134bc5b71e0893e
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#

```

#### Related Commands

|                                 |                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------|
| <a href="#">no</a> on page 1153 | Removes or reverts to default this Bluetooth radio's iBeacon beacon payload parameters |
|---------------------------------|----------------------------------------------------------------------------------------|

#### mode

[interface-config-bluetooth-instance](#) on page 1146

Configures the Bluetooth radio's mode of operation as bt-sensor, le-beacon, or le-sensor.

Supported in the following platforms:

- Access Points - AP7602, AP7612, AP7622, AP7632, AP7662, AP8432, AP8533

#### Syntax

```
mode [bt-sensor | le-beacon | le-sensor]
```

#### Parameters

```
mode [bt-sensor | le-beacon | le-sensor]
```

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mode</b> | <p>Configures the Bluetooth radio's mode of operation. The options are:</p> <ul style="list-style-type: none"> <li>• <b>bt-sensor</b> - Select this option to enable the radio as a bt-sensor. Bt-sensors are Bluetooth classic sensors providing robust wireless connections for legacy devices. Typically these connections are not ideally suited for the newer BLE (Bluetooth low energy) technology supported devices. This is the default setting.</li> <li>• <b>le-beacon</b> - Select this option to provide Bluetooth support for newer BLE technology supported devices. le-beacons are newer Bluetooth low energy beacons ideal for applications requiring intermittent or periodic transfers of small amounts of data. le-beacons are not designed as replacements for classic beacon sensors. If selecting this option, use the <a href="#">beacon</a> on page 1147 keyword to configure the Beacon transmission period and Beacon transmission pattern.</li> <li>• <b>le-sensor</b> - Select this option to provide Bluetooth support for LE (low energy) asset tracking. When enabled, it uses the AP's Bluetooth radio to detect BLE 'asset tags' within the managed network. This information is reported to a back-end server (for example, the NSight server).</li> </ul> |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Example

```

nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#mode le-beacon

nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#show context
interface bluetooth1
 shutdown
 mode le-beacon

```

```
beacon pattern ibeacon
ibeacon calibration-rssi -70
ibeacon major 1110
ibeacon minor 2210
ibeacon uuid f2468da65fa82e841134bc5b71e0893e
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#
```

#### Related Commands

- [no](#) on page 1153 Reverts this Bluetooth radio's mode of operation to le-beacon

## shutdown

[interface-config-bluetooth-instance](#) on page 1146

Shutsdown the selected AP8432/AP8533 Bluetooth radio interface

Supported in the following platforms:

- Access Points - AP7602, AP7612, AP7622, AP7632, AP7662, AP8432, AP8533

#### Syntax

**shutdown**

#### Parameters

None

#### Example

```
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#shutdown

nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#show context
interface bluetooth1
 shutdown
 mode le-beacon
 beacon pattern ibeacon
 ibeacon calibration-rssi -70
 ibeacon major 1110
 ibeacon minor 2210
 ibeacon uuid f2468da65fa82e841134bc5b71e0893e
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#
```

#### Related Commands

- [no](#) on page 1153 Reverses shutdown

## no

[interface-config-bluetooth-instance](#) on page 1146

Removes or reverts to default this AP8432/AP8533 Bluetooth radio interface's settings

Supported in the following platforms:

- Access Points - AP7602, AP7612, AP7622, AP7632, AP7662, AP8432, AP8533

#### Syntax

**no** [beacon | description | eddystone | ibeacon | mode | shutdown]

**no** beacon [pattern | period]

**no** description

```

no eddystone [calibration-rssi|url [1|2]
no ibeacon [calibration-rssi|major|minor|uuid]
no mode
no shutdown

```

Parameters  
no <PARAMETERS>

|                                        |                                                                                                                                                                                                         |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>no</b><br><b>&lt;PARAMETERS&gt;</b> | Removes or reverts to default this Bluetooth radio interface's settings based on the parameters passed <ul style="list-style-type: none"> <li>• &lt;PARAMETERS&gt; - Specify the parameters.</li> </ul> |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Example

The following example shows the AP8432 default profile's Bluetooth radio interface settings:

```

nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#show context
interface bluetooth1
 shutdown
 mode le-beacon
 beacon pattern ibeacon
 ibeacon calibration-rssi -70
 ibeacon major 1110
 ibeacon minor 2210
 ibeacon uuid f2468da65fa82e841134bc5b71e0893e
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#

```

```

nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#no shutdown
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#no ibeacon minor
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#no ibeacon calibration-rssi

```

The following example shows the AP8432 default profile's Bluetooth radio interface settings after the 'no' commands are executed:

```

nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#show context
interface bluetooth1
 no shutdown
 mode le-beacon
 beacon pattern ibeacon
 ibeacon major 1110
 ibeacon uuid f2468da65fa82e841134bc5b71e0893e
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#

```

*ip*

[Profile Config Commands](#) on page 862

The following table summarizes NAT pool configuration commands:

| Command                                               | Description                                                                                                                       |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">ip</a> on page 1155                       | Configures IP components, such as default gateway, DHCP, DNS server forwarding, name server, domain name, routing standards, etc. |
| <a href="#">nat-pool-config-instance</a> on page 1160 | Invokes NAT pool configuration parameters                                                                                         |

## ip

[ip](#) on page 1154

Configures IPv4 routing components, such as default gateway, DHCP, DNS server forwarding, name server, domain name, routing standards, etc.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
ip [default-gateway|dhcp|dns-server-forward|domain-lookup|domain-name|igmp|name-server|nat|route|routing]
```

```
ip default-gateway [<IP>|<HOST-ALIAS-NAME>|failover|priority [dhcp-client <1-1800>|static-route <1-1800>]]
```

```
ip [dns-server-forward|domain-lookup|domain-name <DOMAIN-NAME>|name-server <IP>| routing]
```

```
ip dhcp client [hostname|persistent-lease]
```

```
ip igmp snooping {fast-leave|forward-unknown-multicast|querier}
ip igmp snooping {fast-leave|forward-unknown-multicast}
ip igmp snooping {querier} {max-response-time <1-25>|query-interval <1-18000>|robustness-variable <1-7>|timer expiry <60-300>|version <1-3>}
```



### Note

The command 'ip igmp snooping' can be configured under bridge VLAN context also. For example: rfs7000-37FABE(config-device 00-15-70-37-FA-BE-bridge-vlan-1)#ip igmp snooping forward-unknown-multicast

```
ip nat [crypto|inside|outside|pool]
```

```
ip nat [crypto source pool|pool] <NAT-POOL-NAME>
```

```
ip nat [inside|outside] [destination|source]
```

```
ip nat [inside|outside] destination static <ACTUAL-IP> <1-65535> [tcp|udp] [(<NATTED-IP> {<1-65535>})]
```

```
ip nat [inside|outside] source [list|static]
```

```
ip nat [inside|outside] source static <ACTUAL-IP> <1-65535> [tcp|udp] [(<NATTED-IP> {<1-65535>})]
```

```
ip nat [inside|outside] source list <IP-ACCESS-LIST-NAME> interface
[<INTERFACE-NAME>|pppoe1|vlan <1-4094>|wwan1] [(address <IP>|interface
<L3-IF-NAME>|overload|pool <NAT-POOL-NAME>)]
```

```
ip route <IP/M> [<IP>|<HOST-ALIAS-NAME>]
```

Parameters

```
ip default-gateway [<IP>|<HOST-ALIAS-NAME>|failover|priority [dhcp-client <1-1800>|static-
route <1-1800>]]
```

|                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ip</b>                                                                | Configures IPv4 routing components                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>default-gateway</b>                                                   | Configures default gateway (next-hop router) parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>&lt;IP&gt;</b>                                                        | Configures default gateway's IP address <ul style="list-style-type: none"> <li>&lt;IP&gt; - Specify the default gateway's IP address.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>failover</b>                                                          | Configures failover to the gateway (with next higher priority) when the current default gateway is unreachable (In case of multiple default gateways). This option is enabled by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>&lt;HOST-ALIAS-NAME&gt;</b>                                           | Configures the host alias mapped to the required default gateway <ul style="list-style-type: none"> <li>&lt;HOST-ALIAS-NAME&gt; - Specify the host alias name (should be existing and configured). Host alias names begin with a '\$'.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>priority [dhcp-client &lt;1-1800&gt; static-route &lt;1-1800&gt;]</b> | Configures default gateway priority <ul style="list-style-type: none"> <li>dhcp-client &lt;1-1800&gt; - Defines a priority for the default gateway acquired by the DHCP client on the VLAN interface. The default setting is 1000.</li> <li>static-route &lt;1-1800&gt; - Defines the weight (priority) assigned to this static route versus others that have been defined to avoid potential congestion. The default setting is 100.</li> </ul> <p>The following keyword is common to 'dhcp-client' and 'static-route' parameters:</p> <ul style="list-style-type: none"> <li>&lt;1-1800&gt; - Specify the priority from 1 - 18000 (lower the value higher is the priority).</li> </ul> |

```
ip [dns-server-forward|domain-lookup|domain-name <DOMAIN-NAME>|name-server <IP>|routing]
```

|                                        |                                                                                                                                                                                  |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>• ip</b>                            | Configures IPv4 routing components                                                                                                                                               |
| <b>dns-server-forward</b>              | Enables DNS forwarding. This command enables the forwarding of DNS queries to DNS servers outside of the network. This option is disabled by default.                            |
| <b>domain-lookup</b>                   | Enables domain lookup. When enabled, human friendly domain names are converted into numerical IP destination addresses. The option is enabled by default.                        |
| <b>domain-name &lt;DOMAIN-NAME&gt;</b> | Configures a default domain name <ul style="list-style-type: none"> <li>&lt;DOMAIN-NAME&gt; - Specify a name for the DNS (should not exceed 64 characters in length).</li> </ul> |
| <b>name-server &lt;IP&gt;</b>          | Configures the name server's IP address <ul style="list-style-type: none"> <li>&lt;IP&gt; - Specify the IP address of the name server.</li> </ul>                                |
| <b>routing</b>                         | Enables IP routing of logically addressed packets from their source to their destination. IPv4 routing is enabled by default.                                                    |

```
ip dhcp client [hostname|persistent-lease]
```



|                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ip</b>                                                      | Configures IPv4 routing components                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>dhcp</b>                                                    | Configures the DHCP client and host                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>client</b><br><b>[hostname]</b><br><b>persistent-lease]</b> | Sets the DHCP client <ul style="list-style-type: none"> <li>hostname - Includes the hostname in the DHCP lease for the requesting client. This option is enabled by default.</li> <li>persistent-lease - Retains the last lease across reboots if the DHCP server is unreachable. A persistent DHCP lease assigns the same IP address and other network information to the device each time it renews its DHCP lease. This option is disabled by default.</li> </ul> |

```
ip igmp snooping {fast-leave|forward-unknown-multicast}
```

|                                                |                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ip</b>                                      | Configures IPv4 routing components                                                                                                                                                                                                                                                                                        |
| <b>fast-leave</b>                              | Optional. Enables fast leave processing. When enabled, leave messages are processed quickly, preventing the host from receiving further traffic. Should be configured for one (wired) host network only. This option is disabled by default.<br>This feature is supported only on the AP7502, AP8533 model access points. |
| <b>igmp snooping forward-unknown-multicast</b> | Optional. Enables unknown multicast data packets to be flooded in the specified VLAN. This option is disabled by default.                                                                                                                                                                                                 |

```
ip igmp snooping {querier} {max-response-time <1-25>|query-interval <1-18000>| robustness-variable <1-7>|timer expiry <60-300>|version <1-3>}
```

|                                        |                                                                                                                               |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>ip</b>                              | Configures IPv4 routing components                                                                                            |
| <b>igmp snooping querier</b>           | Optional. Enables the IGMP querier functionality for the specified VLAN. By default IGMP snooping querier is disabled.        |
| <b>max-response-time &lt;1-25&gt;</b>  | Configures the IGMP maximum query response interval used in IGMP V2/V3 queries for the given VLAN. The default is 10 seconds. |
| <b>query-interval &lt;1-18000&gt;</b>  | Configures the IGMP querier query interval in seconds. Specify a value from 1 - 18000 seconds. The default is 60 seconds.     |
| <b>robustness-variable &lt;1-7&gt;</b> | Configures the IGMP robustness variable from 1 - 7. The default is 2.                                                         |
| <b>timer expiry &lt;60-300&gt;</b>     | Configures the other querier time out value for the given VLAN. The default is 60 seconds.                                    |
| <b>version &lt;1-3&gt;</b>             | Configures the IGMP query version for the given VLAN. The default is 3.                                                       |

```
ip nat [crypto source pool|pool <NAT-POOL-NAME>]
```

|            |                                    |
|------------|------------------------------------|
| <b>ip</b>  | Configures IPv4 routing components |
| <b>nat</b> | Configures the NAT parameters      |

|                                                 |                                                                                                                                                                               |
|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>crypto source pool &lt;NAT-POOL-NAME&gt;</b> | Configures the NAT source address translation settings for IPSec tunnels <ul style="list-style-type: none"> <li>• &lt;NAT-POOL-NAME&gt; - Specify a NAT pool name.</li> </ul> |
| <b>pool &lt;NAT-POOL-NAME&gt;</b>               | Configures a pool of IP addresses for NAT <ul style="list-style-type: none"> <li>• &lt;NAT-POOL-NAME&gt; - Specify a name for the NAT pool.</li> </ul>                        |

```
ip nat [inside|outside] destination static <ACTUAL-IP> <1-65535> [tcp|udp] [(<NATTED-IP> {<1-65535>})]
```

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ip</b>                                   | Configures IPv4 routing components                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>nat</b>                                  | Configures the NAT parameters                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>[inside outside]</b>                     | Configures inside and outside address translation for the destination <ul style="list-style-type: none"> <li>• inside - Configures inside address translation</li> <li>• outside - Configures outside address translation</li> </ul>                                                                                                                                                                                               |
| <b>destination static &lt;ACTUAL-IP&gt;</b> | The following keywords are common to the 'inside' and 'outside' parameters: <ul style="list-style-type: none"> <li>• destination - Specifies destination address translation parameters <ul style="list-style-type: none"> <li>• static - Specifies static NAT local to global mapping <ul style="list-style-type: none"> <li>&lt;ACTUAL-IP&gt; - Specify the actual outside IP address to map.</li> </ul> </li> </ul> </li> </ul> |
| <b>&lt;1-65535&gt; [tcp udp]</b>            | <ul style="list-style-type: none"> <li>• &lt;1-65535&gt; - Configures the actual outside port. Specify a value from 1 - 65535.</li> <li>• tcp - Configures Transmission Control Protocol (TCP) port</li> <li>• udp - Configures User Datagram Protocol (UDP) port</li> </ul>                                                                                                                                                       |
| <b>&lt;NATTED-IP&gt; &lt;1-65535&gt;</b>    | Enables configuration of the outside natted IP address <ul style="list-style-type: none"> <li>• &lt;NATTED-IP&gt; - Specify the outside natted IP address. <ul style="list-style-type: none"> <li>• &lt;1-65535&gt; - Optional. Configures the outside natted port. Specify a value from 1 - 65535.</li> </ul> </li> </ul>                                                                                                         |

```
ip nat [inside|outside] source static <ACTUAL-IP> <1-65535> [tcp|udp] [(<NATTED-IP> {<1-65535>})]
```

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ip</b>                              | Configures IPv4 routing components                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>nat</b>                             | Configures the NAT parameters                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>[inside outside]</b>                | Configures inside and outside address translation for the source <ul style="list-style-type: none"> <li>• inside - Configures inside address translation</li> <li>• outside - Configures outside address translation</li> </ul>                                                                                                                                                                                         |
| <b>source static &lt;ACTUAL-IP&gt;</b> | The following keywords are common to the 'inside' and 'outside' parameters: <ul style="list-style-type: none"> <li>• source - Specifies source address translation parameters <ul style="list-style-type: none"> <li>• static - Specifies static NAT local to global mapping <ul style="list-style-type: none"> <li>&lt;ACTUAL-IP&gt; - Specify the actual inside IP address to map.</li> </ul> </li> </ul> </li> </ul> |

|                                                    |                                                                                                                                                                                                                                                                                         |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;1-65535&gt;</b><br><b>[tcp udp]</b>         | <ul style="list-style-type: none"> <li>• &lt;1-65535&gt; - Configures the actual outside port. Specify a value from 1 - 65535.</li> <li>• tcp - Configures Transmission Control Protocol (TCP) port</li> <li>• udp - Configures User Datagram Protocol (UDP) port</li> </ul>            |
| <b>&lt;NATTED-IP&gt;</b><br><b>&lt;1-65535&gt;</b> | <p>Enables configuration of the outside natted IP address</p> <ul style="list-style-type: none"> <li>• &lt;NATTED-IP&gt; - Specify the outside natted IP address.</li> <li>• &lt;1-65535&gt; - Optional. Configures the outside natted port. Specify a value from 1 - 65535.</li> </ul> |

```
ip nat [inside|outside] source list <IP-ACCESS-LIST-NAME> interface [<INTERFACE-NAME>|
pppoe1|vlan <1-4094>|wwan1] [(address <IP>|interface <L3-IF-NAME>|overload] pool <NAT-POOL-
NAME>)]
```

|                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ip</b>                                                                              | Configures IPv4 routing components                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>nat</b>                                                                             | Configures the NAT parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>[inside outside]</b>                                                                | Configures inside and outside IP access list                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>source list</b><br><b>&lt;IP-ACCESS-LIST-NAME&gt;</b>                               | <p>Configures an access list describing local addresses</p> <ul style="list-style-type: none"> <li>• &lt;IP-ACCESS-LIST-NAME&gt; - Specify a name for the IP access list.</li> </ul>                                                                                                                                                                                                                                                                                                                                   |
| <b>interface</b><br><b>[&lt;INTERFACE-NAME&gt;  pppoe1 vlan &lt;1-4094&gt;  wwan1]</b> | <p>Selects an interface to configure. Select a layer 3 router interface or a VLAN interface.</p> <ul style="list-style-type: none"> <li>• &lt;INTERFACE-NAME&gt; - Selects a layer 3 interface. Specify the layer 3 router interface name.</li> <li>• vlan - Selects a VLAN interface <ul style="list-style-type: none"> <li>• &lt;1-4094&gt; - Set the SVI VLAN ID of the interface.</li> </ul> </li> <li>• pppoe1 - Selects PPP over Ethernet interface</li> <li>• wwan1 - Selects Wireless WAN interface</li> </ul> |
| <b>address &lt;IP&gt;</b>                                                              | <p>The following keyword is recursive and common to all interface types:</p> <ul style="list-style-type: none"> <li>• address &lt;IP&gt; - Configures the interface IP address used with NAT</li> </ul>                                                                                                                                                                                                                                                                                                                |
| <b>interface &lt;L3-IF-NAME&gt;</b>                                                    | <p>The following keyword is recursive and common to all interface types:</p> <ul style="list-style-type: none"> <li>• interface &lt;L3-IF-NAME&gt; - Configures a wireless controller or service platform's VLAN interface <ul style="list-style-type: none"> <li>• &lt;L3IFNAME&gt; - Specify the SVI VLAN ID of the interface.</li> </ul> </li> </ul>                                                                                                                                                                |
| <b>overload</b>                                                                        | <p>The following keyword is recursive and common to all interface types:</p> <ul style="list-style-type: none"> <li>• overload - Enables use of global address for many local addresses</li> </ul>                                                                                                                                                                                                                                                                                                                     |
| <b>pool &lt;NAT-POOL-NAME&gt;</b>                                                      | <p>The following keyword is recursive and common to all interface types:</p> <ul style="list-style-type: none"> <li>• pool &lt;NAT-POOL-NAME&gt; - Specifies the NAT pool <ul style="list-style-type: none"> <li>• &lt;NAT-POOL-NAME&gt; - Specify the NAT pool name.</li> </ul> </li> </ul>                                                                                                                                                                                                                           |

```
ip route <IP/M> [<IP>|<HOST-ALIAS-NAME>]
```

|                     |                                                            |
|---------------------|------------------------------------------------------------|
| <b>ip</b>           | Configures IPv4 routing components                         |
| <b>route</b>        | Configures the static routes                               |
| <b>&lt;IP/M&gt;</b> | Specify the IP destination prefix in the A.B.C.D/M format. |

|                                |                                                                                                                                                                                                                                                     |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;IP&gt;</b>              | Specify the IP address of the gateway.                                                                                                                                                                                                              |
| <b>&lt;HOST-ALIAS-NAME&gt;</b> | Configures the host alias mapped to the required default gateway <ul style="list-style-type: none"> <li>• &lt;HOST-ALIAS-NAME&gt; - Specify the host alias name (should be existing and configured). Host alias names begin with a '\$'.</li> </ul> |

### Example

```
NOC-NX9500(config-profile-testNX9000)#ip default-gateway 10.234.160.5
NOC-NX9500(config-profile-testNX9000)#ip dns-server-forward
NOC-NX9500(config-profile-testNX9000)#ip nat inside source list BROADCAST-MULTIC
AST-CONTROL precedence 1 interface vlan 1 pool NATPool1 overload
```

```
NOC-NX9500(config-profile-testNX9000-nat-pool-NATPool1)#?
```

Nat Policy Mode commands:

```
address Specify addresses for the nat pool
no Negate a command or set its defaults

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal
```

```
NOC-NX9500(config-profile-testNX9000-nat-pool-NATPool1)#
```

### Related Commands

|                        |                                               |
|------------------------|-----------------------------------------------|
| <b>no</b> on page 1200 | Disables or reverts settings to their default |
|------------------------|-----------------------------------------------|

## nat-pool-config-instance

**ip** on page 1154

Use the config-profile-<DEVICE-PROFILE-NAME> instance to configure Network Address Translation (NAT) pool settings.

The following example uses the config-profile-nx9500-6C8809 instance to configure NAT pool settings:

```
nx9500-6C8809(config-profile-default-rfs4000)#ip nat pool pool1
nx9500-6C8809(config-profile-default-rfs4000-nat-pool-pool1)#
```

```
nx9500-6C8809(config-profile-default-rfs4000-nat-pool-pool1)#?
```

Nat Policy Mode commands:

```
address Specify addresses for the nat pool
no Negate a command or set its defaults

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
```

```
show Show running system information
write Write running configuration to memory or terminal
```

```
nx9500-6C8809(config-profile-default-rfs4000-nat-pool-pool1)
```

The following table summarizes NAT pool configuration commands:

| Command                              | Description                           |
|--------------------------------------|---------------------------------------|
| <a href="#">address</a> on page 1161 | Configures NAT pool addresses         |
| <a href="#">no</a> on page 1162      | Negates a command or sets its default |

## address

[nat-pool-config-instance](#) on page 1160

Configures NAT pool of IP addresses

Define a range of IP addresses hidden from the public Internet. NAT modifies network address information in the defined IP range while in transit across a traffic routing device. NAT only provides IP address translation and does not provide a firewall. A branch deployment with NAT by itself will not block traffic from being potentially routed through a NAT device. Consequently, NAT should be deployed with a stateful firewall.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

### Syntax

```
address [<IP> | range <START-IP> <END-IP>]
```

### Parameters

```
address [<IP> | range <START-IP> <END-IP>]
```

|                                              |                                                                                                                                                                                                                                        |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>address &lt;IP&gt;</b>                    | Adds a single IP address to the NAT pool                                                                                                                                                                                               |
| <b>range &lt;START-IP&gt; &lt;END-IP&gt;</b> | Adds a range of IP addresses to the NAT pool <ul style="list-style-type: none"><li>• &lt;START-IP&gt; - Specify the starting IP address of the range.</li><li>• &lt;END-IP&gt; - Specify the ending IP address of the range.</li></ul> |

### Example

```
nx9500-6C8809(config-profile-default-rfs4000-nat-pool-pool1)#address range 172.16.10.2 172.16.10.8
```

```
nx9500-6C8809(config-profile-default-rfs4000-nat-pool-pool1)#show context
ip nat pool pool1
address range 172.16.10.2 172.16.10.8
nx9500-6C8809(config-profile-default-rfs4000-nat-pool-pool1)#
```

### Related Commands

|                                 |                                                   |
|---------------------------------|---------------------------------------------------|
| <a href="#">no</a> on page 1200 | Removes address(es) configured with this NAT pool |
|---------------------------------|---------------------------------------------------|

no

[nat-pool-config-instance](#) on page 1160

Removes address(es) configured with this NAT pool

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
no address [<IP>|range <START-IP> <END-IP>]
```

Parameters

```
no address [<IP>|range <START-IP> <END-IP>]
```

|                                                                                                                                                                                                       |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre><b>no address</b>           Removes a single IP address or a range of IP addresses from this NAT pool<br/><b>[&lt;IP&gt;  range</b><br/><b>&lt;START-IP&gt;</b><br/><b>&lt;END-IP&gt;]</b></pre> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Usage Guidelines

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
nx9500-6C8809(config-profile-default-rfs4000-nat-pool-pool1)#show context
 ip nat pool pool1
 address range 172.16.10.2 172.16.10.8
nx9500-6C8809(config-profile-default-rfs4000-nat-pool-pool1)#

nx9500-6C8809(config-profile-default-rfs4000-nat-pool-pool1)#no address range 1
72.16.10.2 172.16.10.8

nx9500-6C8809(config-profile-default-rfs4000-nat-pool-pool1)#show context
 ip nat pool pool1
nx9500-6C8809(config-profile-default-rfs4000-nat-pool-pool1)#
```

Related Commands

|                                                                                    |
|------------------------------------------------------------------------------------|
| <p><a href="#">address</a> on page 1161     Configures NAT pool IP address(es)</p> |
|------------------------------------------------------------------------------------|

*ipv6*

[Profile Config Commands](#) on page 862

Configures IPv6 routing components, such as default gateway, DNS server forwarding, name server, routing standards, etc.

These IPv6 settings are applied to all devices using this profile.

You can also configure IPv6 settings on a device, using the device's configuration mode.

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600



#### Note

The IPv6 settings configured at the profile/device level are global configuration settings and not interface-specific.

### Syntax

```
ipv6 [default-gateway|dns-server-forward|hop-limit|mld|name-server|nd-reachable-time|neighbor|ns-interval|ra-convert|route|ula-reject-route|unicast-routing]
```

```
ipv6 [default-gateway <IPv6> {vlan <VLAN-ID>}/dns-server-forward|hop-limit <1-255>|name-server <IPv6>|nd-reachable-time <5000-3600000>|ns-interval <1000-3600000>|ula-reject-route|unicast-routing]
```

```
ipv6 ra-convert {throttle interval <3-1800> max-RAs <1-256>}
```

```
ipv6 mld snooping {forward-unknown-multicast|querier}
ipv6 mld snooping {forward-unknown-multicast}
ipv6 mld snooping {querier} {max-response-time <1-25000>|query-interval <1-18000>|robustness-variable <1-7>|timer expiry <60-300>|version <1-2>}
```

```
ipv6 neighbor [<IPv6>|timeout]
```

```
ipv6 neighbor <IPv6> <MAC> [<INTF-NAME>|pppoe1|vlan <1-4094>|wwan1]
{dhcp-server| router}
ipv6 neighbor timeout <15-86400>
```

```
ipv6 route <DEST-IPv6-PREFIX/PREFIX-LENGTH> <IPv6-GATEWAY-ADDRESS> {vlan <VLAN-ID>}
```

### Parameters

```
ipv6 [default-gateway <IPv6> {vlan <VLAN-ID>}|dns-server-forward|hop-limit <1-255>|name-server <IPv6>|nd-reachable-time <5000-3600000>|ns-interval <1000-3600000>|ula-reject-route|unicast-routing]
```

|                                                            |                                                                                                                                                                                                                                  |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipv6</b>                                                | Configures IPv6 routing components                                                                                                                                                                                               |
| <b>default-gateway &lt;IPv6&gt; {vlan &lt;VLAN-ID&gt;}</b> | Configures IPv6 default gateway's address in the ::/0 format <ul style="list-style-type: none"><li>• vlan &lt;VLAN-ID&gt; - Optional. Specify the VLAN interface's ID through which the default gateway is accessible.</li></ul> |
| <b>dns-server-forward</b>                                  | Enables DNS server forwarding. This command enables the forwarding of DNS queries to DNS servers outside of the network. This feature is disabled by default.                                                                    |

|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>hop-limit</b><br><b>&lt;1-255&gt;</b>                | Configures the IPv6 hop count limit <ul style="list-style-type: none"> <li>• &lt;1-255&gt; – Specify a value between 1 - 255. The default is 64.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>name-server</b><br><b>&lt;IPv6&gt;</b>               | Configures the IPv6 name server's address <ul style="list-style-type: none"> <li>• &lt;IPv6&gt; – Specify the address of the IPv6 name server.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>nd-reachable-time</b><br><b>&lt;5000-3600000&gt;</b> | Configures the time, in milliseconds, that a neighbor is assumed to be reachable after having received neighbor discovery (ND) confirmation for their reachability <ul style="list-style-type: none"> <li>• &lt;5000-3600000&gt; – Specify a value from 5000 - 3600000 milliseconds. The default is 30,000 milliseconds.</li> </ul>                                                                                                                                                                                                                                                                                               |
| <b>ns-interval</b><br><b>&lt;1000-3600000&gt;</b>       | Configures the interval, in milliseconds, between two consecutive retransmitted neighbor solicitation (NS) messages. NS messages are sent by a node to determine the link layer address of a neighbor, or verify a neighbor is still reachable via a cached link-layer address. <ul style="list-style-type: none"> <li>• &lt;1000-3600000&gt; – Specify a value from 1000 - 3600000. The default is 1000 milliseconds.</li> </ul>                                                                                                                                                                                                 |
| <b>ula-reject-route</b>                                 | Installs a "reject" route for Unique Local Address (ULA) prefixes. This ensures that site-border routers and firewalls do not forward packets with ULA source or destination addresses outside of the site, unless explicitly configured with routing information about specific /48 or longer Local IPv6 prefixes. This option is disabled by default. The ULA is an IPv6 address used in private networks for local communication within a site (for example a company, campus, or within a set of branch office networks). These site local addresses are IPv6 addresses that fall in the block fc00::/7, defined in RFC 4193. |
| <b>unicast-routing</b>                                  | Enables IPv6 unicast routing. This feature is enabled by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

```
ipv6 ra-convert {throttle interval <3-1800> max-RAs <1-256>}
```

|                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipv6</b>                                                                                                         | Configures IPv6 routing components                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>ra-convert</b><br><b>{throttle</b><br><b>interval</b><br><b>&lt;3-1800&gt; max-</b><br><b>RAAs &lt;1-256&gt;</b> | Enables conversion of multicast router advertisements (RAs) to unicast RAs at the dot11 layer. This feature is disabled by default. <ul style="list-style-type: none"> <li>• throttle – Optional. Throttles multicast RAs before converting to unicast</li> <li>• interval &lt;3-1800&gt; – Throttles multicast RAs for a specified time period. Specify the interval from 3 - 1800 seconds. The default is 3 seconds.</li> <li>• max-RAs &lt;1-256&gt; – Specifies the maximum number of RAs per IPv6 router during the specified throttle interval. Specify a value from 1 - 256. The default is 1.</li> </ul> |

```
ipv6 mld snooping {forward-unknown-multicast}
```



|                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipv6</b>                                   | Configures IPv6 routing components                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>mld snooping forward-unknown-multicast</b> | <p>Enables multicast listener discovery (MLD) protocol snooping. This feature is disabled by default.</p> <p>When enabled, IPv6 devices (access point, wireless controller, or service platform) can examine MLD messages exchanged between hosts and multicast routers to discern which hosts are receiving multicast group traffic. Based on the information gathered these devices forward multicast traffic only to those interfaces connected to interested receivers instead of flooding traffic to all interfaces. This prevents VLANs from getting flooded with IPv6 multicast traffic.</p> |
|                                               | <ul style="list-style-type: none"> <li>forward-unknown-multicast – Optional. Enables unknown multicast forwarding. This feature is enabled by default.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                   |

```
ipv6 mld snooping {querier} {max-response-time <1-25000>|query-interval <1-18000>|robustness-variable <1-7>|timer expiry <60-300>|version <1-2>}
```

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipv6</b>                              | Configures IPv6 routing components                                                                                                                                                                                                                                                                                                                                                              |
| <b>mld snooping querier</b>              | <p>Enables MLD protocol snooping</p> <ul style="list-style-type: none"> <li>querier – Optional. Enables the on-board MLD querier. When enabled, IPv6 devices send query messages to discover which network devices are members of a given multicast group. This option is disabled by default.</li> </ul>                                                                                       |
| <b>max-response-time &lt;1-25000&gt;</b> | <p>Configures the MLD querier's maximum query response time. This is the time for which the querier waits before sending a responding report. Queriers use MLD reports to join and leave multicast groups and receive group traffic.</p> <ul style="list-style-type: none"> <li>&lt;1-25000&gt; – Specify a value from 1 - 25000 milliseconds. The default is 10 milliseconds.</li> </ul>       |
| <b>query-interval &lt;1-18000&gt;</b>    | <p>Configures the interval, in seconds, between two consecutive MLD querier's queries. The robustness variable is an indication of how susceptible the subnet is to lost packets. MLD can recover from robustness variable minus 1 lost MLD packets.</p> <ul style="list-style-type: none"> <li>&lt;1-18000&gt; – Specify a value from 1 - 18000 seconds. The default is 60 seconds.</li> </ul> |
| <b>robustness-variable &lt;1-7&gt;</b>   | <p>Configures the MLD IGMP robustness variable. This value is used by the sender of a query.</p> <ul style="list-style-type: none"> <li>&lt;1-7&gt; – Select a value from 1 - 7. The default is 2.</li> </ul>                                                                                                                                                                                   |
| <b>timer expiry &lt;60-300&gt;</b>       | <p>Configures the MLD other querier (any external querier) timeout</p> <ul style="list-style-type: none"> <li>&lt;60-300&gt; – Specify a value from 60 - 300 seconds. The default is 60 seconds.</li> </ul>                                                                                                                                                                                     |
| <b>version &lt;1-2&gt;</b>               | <p>Configures the MLD querier's version. MLD version 1 is based on IGMP version 2 for IPv4. MLD version 2 is based on IGMP version 3 for IPv4 and is fully backward compatible. IPv6 multicast uses MLD version 2.</p> <ul style="list-style-type: none"> <li>&lt;1-2&gt; – Select the MLD version from 1 - 2. The default is 2.</li> </ul>                                                     |

```
ipv6 neighbor <IPv6> <MAC> [<INTF-NAME>|pppoe1|vlan <1-4094>|wwan1] {dhcp-server|router}
```

|                     |                                                                        |
|---------------------|------------------------------------------------------------------------|
| <b>ipv6</b>         | Configures IPv6 routing components                                     |
| <b>neighbor</b>     | Configures static IPv6 neighbor entries                                |
| <b>&lt;IPv6&gt;</b> | Specify the IPv6 address for which a static neighbor entry is created. |
| <b>&lt;MAC&gt;</b>  | Specify the MAC address associated with the specified IPv6 address.    |

|                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[ &lt;INTF-NAME&gt;   pppoe1   vlan &lt;1-4094&gt;   wwan1 ]</b> | Specify the following interface settings: <ul style="list-style-type: none"> <li>• &lt;INTF-NAME&gt; - Selects the layer 3 router interface. Specify the interface name.</li> <li>• pppoe1 - Selects the PPP over Ethernet interface</li> <li>• vlan &lt;1-4094&gt; - Selects the VLAN interface. Specify the VLAN interface index.</li> <li>• wwan1 - Selects the wireless WAN interface</li> </ul> |
| <b>{ dhcp-server   router }</b>                                     | After specifying interface type, you can optionally specify the device type for this neighbor solicitation. <ul style="list-style-type: none"> <li>• dhcp-server - Optional. States this neighbor entry is for a DHCP server</li> <li>• router - Optional. States this neighbor entry is for a router</li> </ul>                                                                                     |

```
ipv6 neighbor timeout <15-86400>
```

|                                 |                                                                                                                                                                                                                  |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>neighbor</b>                 | Configures static IPv6 neighbor entries                                                                                                                                                                          |
| <b>timeout &lt;15-86400&gt;</b> | Configures the timeout, in seconds, for the static neighbor entries <ul style="list-style-type: none"> <li>• &lt;15-86400&gt; - Specify a value from 15 - 86400 seconds. The default is 3600 seconds.</li> </ul> |

```
ipv6 route <DEST-IPv6-PREFIX/PREFIX-LENGTH> <IPv6-GATEWAY-ADDRESS> {vlan <VLAN-ID>}
```

|                                               |                                                                                                                                                                                               |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipv6</b>                                   | Configures IPv6 routing components                                                                                                                                                            |
| <b>route</b>                                  | Configures the static routes<br>These routes are maintained in the IPv6 Forwarding Information Base (FIB).<br>To view FIB6 routing entries, use the service > show fib6 > <TABLE-ID> command. |
| <b>&lt;DEST-IPv6-PREFIX/PREFIX-LENGTH&gt;</b> | Specify the IPv6 destination prefix (IPv6 network) and the prefix length.                                                                                                                     |
| <b>&lt;IPv6-GATEWAY-ADDRESS&gt;</b>           | Specify the IPv6 gateway's address.                                                                                                                                                           |
| <b>vlan &lt;VLAN-ID&gt;</b>                   | Optional. specify the VLAN interface's ID (through which the default gateway is accessible)<br>This parameter is needed only if the gateway address is a link local address.                  |

### Example

```
nx9500-6C8809(config-profile-TestRFS4000)#ipv6 default-gateway 2001:10:10:10:10:10:2

nx9500-6C8809(config-profile-TestRFS4000)#ipv6 dns-server-forward

nx9500-6C8809(config-profile-TestRFS4000)#ipv6 mld snooping

nx9500-6C8809(config-profile-TestRFS4000)#show context
profile rfs4000 TestRFS6000
 ipv6 mld snooping
 ipv6 dns-server-forward
 ipv6 default-gateway 2001:10:10:10:10:10:2
 no autoinstall configuration
 no autoinstall firmware
 crypto ikev1 policy ikev1-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
 --More--
nx9500-6C8809(config-profile-TestRFS4000)#
```

## Related Commands

|                              |                                                    |
|------------------------------|----------------------------------------------------|
| <code>no</code> on page 1200 | Disables or reverts IPv6 settings to their default |
|------------------------------|----------------------------------------------------|

### *l2tpv3*

[Profile Config Commands](#) on page 862

Defines the L2TPV3 settings for tunneling layer 2 payloads using VPNs

L2TPv3 is an IETF standard that defines the control and encapsulation protocol settings for tunneling layer 2 frames in an IP network (and access point profile) between two IP nodes. Use L2TPv3 to create tunnels for transporting layer 2 frames. L2TPv3 enables WiNG supported controllers and access points to create tunnels for transporting Ethernet frames to and from bridge VLANs and physical ports. L2TPv3 tunnels can be defined between WiNG devices and other vendor devices supporting the L2TPv3 protocol.

#### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

#### Syntax

```
l2tpv3 [hostname <HOSTNAME> | inter-tunnel-bridging | logging | manual-session |
router-id [<1-4294967295> | <IP>] | tunnel | udp-listen-port <1024-65535>]
```

```
l2tpv3 logging ip-address [<IP> | any] hostname [<HOSTNAME> | any] router-id
[<IP> | <WORD> | any]
```

#### Parameters

```
l2tpv3 [hostname <HOSTNAME> | inter-tunnel-bridging | manual-session | router-id [<1-4294967295> |
<IP>] | tunnel | udp-listen-port <1024-65535>]
```

|                                                                |                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>l2tpv3</b>                                                  | Configures the L2TPv3 protocol settings for a profile                                                                                                                                                                                                                                                                                                                 |
| <b>hostname</b><br><b>&lt;HOSTNAME&gt;</b>                     | Configures the host name sent in the L2TPv3 signalling messages. Tunnel establishment involves exchanging 3 message types (SCCRQ, SCCRP and SCCN) with the peer. Tunnel IDs and capabilities are exchanged during the tunnel establishment with the host. <ul style="list-style-type: none"><li>• &lt;HOSTNAME&gt; - Specify the L2TPv3 specific host name.</li></ul> |
| <b>inter-tunnel-bridging</b>                                   | Enables inter tunnel bridging of packets. This feature is disabled by default.                                                                                                                                                                                                                                                                                        |
| <b>manual-session</b>                                          | Creates/modifies L2TPv3 manual sessions<br>For more information, see <a href="#">l2tpv3-manual-session-commands</a> on page 1714.                                                                                                                                                                                                                                     |
| <b>router-id</b><br><b>[&lt;1-4294967295&gt;   &lt;IP&gt;]</b> | Configures the router ID sent in the L2TPv3 signaling messages. These signaling (AVP) messages help to identify tunneled peers. <ul style="list-style-type: none"><li>• &lt;1-4294967295&gt; - Configures the router ID in decimal format from 1 - 4294967295</li><li>• &lt;IP&gt; - Configures the router ID in the IP address (A.B.C.D) format</li></ul>            |

|                                                     |                                                                                                                                                                                               |
|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>tunnel</b>                                       | Creates/modifies an L2TPv3 tunnel<br>For more information, see <a href="#">l2tpv3-tunnel-commands</a> on page 1700.                                                                           |
| <b>udp-listen-port</b><br><b>&lt;1024-65535&gt;</b> | Configures the UDP port used to listen for incoming traffic <ul style="list-style-type: none"> <li>• &lt;1024-65535&gt; - Specify the UDP port from 1024 - 65535 (default is 1701)</li> </ul> |

`l2tpv3 logging ip-address [<IP>|any] hostname [<HOSTNAME>|any] router-id [<IP>|<WORD>|any]`

|                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>l2tpv3</b>                                            | Configures L2TPv3 protocol settings for a profile                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>logging</b>                                           | Enables L2TPv3 tunnel event logging and debugging. When enabled, all events relating to Ethernet frames to and from bridge VLANs and physical ports on a specified IP address, host or router ID are logged. This option is disabled by default.                                                                                                                                                                                          |
| <b>ip-address</b><br><b>[&lt;IP&gt; any]</b>             | Configures the L2TPv3 peer tunnel IP address for which event logging is enabled. The options are: <ul style="list-style-type: none"> <li>• &lt;IP&gt; - Specify the peer's IP address. L2TPv3 events are captured and logged for the specified peer.</li> <li>• any - Peer's IP address is not specified. Enables event logging for all incoming connections from any IP address.</li> </ul>                                              |
| <b>hostname</b><br><b>[&lt;HOSTNAME&gt; any]</b>         | Configures the L2TPv3 peer tunnel hostname for which event logging is enabled. The options are: <ul style="list-style-type: none"> <li>• &lt;HOSTNAME&gt; - Specify the peer's host name. L2TPv3 events are captured and logged for specified host.</li> <li>• any - Peer's hostname is not specified. Enables debugging for all incoming connections from any host.</li> </ul>                                                           |
| <b>router-id</b><br><b>[&lt;IP&gt; &lt;WORD&gt; any]</b> | Configures the L2TPv3 tunnel router ID for which event logging is enabled. The options are: <ul style="list-style-type: none"> <li>• &lt;IP&gt; - Specify the router ID in the IP address format.</li> <li>• &lt;WORD&gt; - Specify the router ID in the form of an integer or range. For example 100-200.</li> <li>• any - Router ID is not specified. Enables debugging for all incoming connections from any L2TPv3 router.</li> </ul> |

### Example

```

nx9500-6C8809(config-profile-default-rfs4000)#l2tpv3 hostname l2tpv3Host1

nx9500-6C8809(config-profile-default-rfs4000)#l2tpv3 inter-tunnel-bridging

nx9500-6C8809(config-profile-default-rfs4000)#show context
profile rfs4000 default-rfs4000
 bridge vlan 1
 bridging-mode isolated-tunnel
 ip igmp snooping
 ip igmp snooping querier

 l2tpv3 hostname l2tpv3Host1
 l2tpv3 inter-tunnel-bridging
nx9500-6C8809(config-profile-default-rfs4000)#

```

### Related Commands

|                        |                                                  |
|------------------------|--------------------------------------------------|
| <b>no</b> on page 1200 | Negates a L2TPv3 tunnel settings on this profile |
|------------------------|--------------------------------------------------|

## *l3e-lite-table*

[Profile Config Commands](#) on page 862

Configures L3e lite table aging time

The L3e Lite table stores information about destinations and their location within a specific IPsec tunnel. This enables quicker packet transmissions. The table is updated as nodes transmit packets.

### **Supported in the following platforms:**

- Wireless Controllers — RFS4000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

### **Syntax**

```
l3e-lite-table aging-time <10-1000000>
```

### **Parameters**

```
l3e-lite-table aging-time <10-1000000>
```

|                           |                                                                                                                                                                                                             |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>l3e-lite-table</b>     | Configures the aging time in seconds. The aging time defines the duration a learned L3e entry (IP, VLAN) remains in the L3e Lite table before deletion due to lack of activity. The default is 300 seconds. |
| <b>aging-time</b>         |                                                                                                                                                                                                             |
| <b>&lt;10-1000000&gt;</b> |                                                                                                                                                                                                             |

### **Example**

```
nx9500-6C8809(config-profile-default-rfs4000)#l3e-lite-table aging-time 1000
```

```
nx9500-6C8809(config-profile-default-rfs4000)#show context
profile rfs7000 default-rfs4000
 bridge vlan 1
 bridging-mode isolated-tunnel
 ip igmp snooping
 ip igmp snooping querier

 interface ge4
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
 interface pppoe1
 use firewall-policy default
 l3e-lite-table aging-time 1000
 --More--
nx9500-6C8809(config-profile-default-rfs4000)#
```

### **Related Commands**

|                        |                                                     |
|------------------------|-----------------------------------------------------|
| <b>no</b> on page 1200 | Removes the L3e lite table aging time configuration |
|------------------------|-----------------------------------------------------|

## *led*

[Profile Config Commands](#) on page 862

Turns on and off access point LEDs

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

### Syntax

```
led {flash-pattern}
```

### Parameters

```
led {flash-pattern}
```

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>led flash-pattern</b> | Optional. Enables LED flashing on the device using this profile<br>Select this option to flash an access point's LEDs in a distinct manner (different from its operational LED behavior). Enabling this feature allows an administrator to validate an access point has received its configuration (perhaps remotely at the site of deployment) without having to log into the managing controller or service platform. This feature is disabled by default. |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Example

```
nx9500-6C8809(config-profile-RFS6000Test)#led flash-pattern

nx9500-6C8809(config-profile-RFS6000Test)#show context
profile rfs4000 RFS4000Test
no autoinstall configuration
no autoinstall firmware
led flash-pattern
crypto ikev1 policy ikev1-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ikev2 policy ikev2-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
crypto ikev1 remote-vpn
crypto ikev2 remote-vpn
crypto auto-ipsec-secure
--More--
nx9500-6C8809(config-profile-RFS4000Test)#
```

### Related Commands

|                                 |                                               |
|---------------------------------|-----------------------------------------------|
| <a href="#">no</a> on page 1200 | Disables or reverts settings to their default |
|---------------------------------|-----------------------------------------------|

### *led-timeout*

[Profile Config Commands](#) on page 862

Configures the LED-timeout timer in the device or profile configuration mode

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

## Syntax

```
led-timeout [<15-1440>|shutdown]
```

## Parameters

```
led-timeout [<15-1440>|shutdown]
```

**led-time**  
**[<15-1440>|**  
**shutdown]**

Sets the LED-timeout timer. The value provided here determines the interval (time to lapse) for which a device's LEDs are turned off after the last radio state change. For example, if set at 15 minutes, the LEDs are turned off for 15 minutes after the last radio state change.

- <15-1440> – Specify a value from 15 - 1400 minutes. The default is 30 minutes.
- shutdown – Shuts down the LED-timeout timer. The device LEDs are not turned off.

## Example

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#led-timeout 25
```

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context
```

```
nx9000 B4-C7-99-6C-88-09
 use profile default-nx9000
 use rf-domain default
 hostname nx9500-6C8809
 license AAP
66069c24b3bb1259b34ff016c723a9e299dd408f0ff891e7c5f7e279a382648397d6b3e975e356a1
 license HTANLT
66069c24b3bb1259eb36826cab3cc83999dd408f0ff891e74b62b2d3594f0b3dde7967f30e49e497
 no autogen-uniqueid
 ip default-gateway 192.168.13.2
 led-timeout 25
 --More--
```

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#led-timeout shutdown
```

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context
```

```
nx9000 B4-C7-99-6C-88-09
 use profile default-nx9000
 use rf-domain default
 hostname nx9500-6C8809
 license AAP
66069c24b3bb1259b34ff016c723a9e299dd408f0ff891e7c5f7e279a382648397d6b3e975e356a1
 license HTANLT
66069c24b3bb1259eb36826cab3cc83999dd408f0ff891e74b62b2d3594f0b3dde7967f30e49e497
 no autogen-uniqueid
 ip default-gateway 192.168.13.2
 led-timeout shutdown
 crypto ikev2 peer IKEv2Peer1
 --More--
```

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```

## Related Commands

|                              |                            |
|------------------------------|----------------------------|
| <code>no</code> on page 1200 | Disables LED-timeout timer |
|------------------------------|----------------------------|

*legacy-auto-downgrade*

[Profile Config Commands](#) on page 862

Enables device firmware to auto downgrade when legacy devices are detected

**Supported in the following platforms:**

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

**Syntax**

legacy-auto-downgrade

**Parameters**

None

**Example**

```
nx9500-6C8809(config-profile-default-rfs4000)#legacy-auto-downgrade
```

**Related Commands**

|                                 |                                                                                 |
|---------------------------------|---------------------------------------------------------------------------------|
| <a href="#">no</a> on page 1200 | Prevents device firmware from auto downgrading when legacy devices are detected |
|---------------------------------|---------------------------------------------------------------------------------|

*legacy-auto-update*

[Profile Config Commands](#) on page 862

Auto updates an AP7161 legacy access point firmware

**Supported in the following platforms:**

- Access Points — AP7161

**Syntax**

legacy-auto-update ap71xx image <FILE>]

**Parameters**

legacy-auto-update ap71xx image <FILE>

|                                  |                                                                                                                                                                                                                       |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>legacy-auto-update</b>        | Updates a legacy AP7161 access point firmware                                                                                                                                                                         |
| <b>ap71xx image &lt;FILE&gt;</b> | Auto updates legacy AP7161 firmware <ul style="list-style-type: none"><li>• image - Sets the path to the firmware image</li><li>• &lt;FILE&gt; - Specify the path and filename in the flash:/ap.img format.</li></ul> |

**Example**

```
nx9500-6C8809(config-profile-default-rfs4000)#legacy-auto-update ap71xx image flash:/ap47d.img
```





## Related Commands

|                              |                                            |
|------------------------------|--------------------------------------------|
| <code>no</code> on page 1200 | Disables automatic legacy firmware upgrade |
|------------------------------|--------------------------------------------|

*lldp*

[Profile Config Commands](#) on page 862

Enables LLDP on this profile and configures LLDP settings

LLDP or IEEE 802.1AB is a vendor-neutral Data Link Layer protocol used by network devices for advertising of (announcing) identity, capabilities, and interconnections on a IEEE 802 LAN network. The protocol is formally referred to by the IEEE as Station and Media Access Control Connectivity Discovery. Both LLDP snooping and ability to generate and transmit LLDP packets is provided.

Information obtained via CDP and LLDP snooping is available in the UI. Information obtained using LLDP is provided during the adoption process, so the layer 2 device detected by the access point can be used as a criteria in the provisioning policy.

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
lldp [holdtime | med-tlv-select | run | timer]
```

```
lldp [holdtime <10-1800> | run | timer <5-900>]
```

```
lldp med-tlv-select [inventory-management | power-management {auto}]
```

### Parameters

```
lldp [holdtime <10-1800> | run | timer <5-900>]
```

|                                           |                                                                                                                                                                                                                                                                                 |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>lldp</b>                               | Enables LLDP on this profile and configures LLDP settings                                                                                                                                                                                                                       |
| <b>holdtime</b><br><b>&lt;10-1800&gt;</b> | Sets the holdtime for transmitted LLDP PDUs. This command specifies the time a receiving device holds information before discarding. <ul style="list-style-type: none"><li>• &lt;10-1800&gt; - Specify a holdtime from 10 - 1800 seconds. The default is 180 seconds.</li></ul> |
| <b>run</b>                                | Enables LLDP on this profile                                                                                                                                                                                                                                                    |
| <b>timer</b> <b>&lt;5-900&gt;</b>         | Sets the transmit interval. This command specifies the transmission frequency of LLDP updates in seconds. <ul style="list-style-type: none"><li>• &lt;5-900&gt; - Specify transmit interval from 5 - 900 seconds. The default is 60 seconds.</li></ul>                          |

```
lldp med-tlv-select [inventory-management | power-management {auto}]
```

|                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>lldp</b>                                                                                                                | Enables LLDP on this profile and configures LLDP settings                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>med-tlv-select</b><br><b>[inventory-</b><br><b>management  </b><br><b>power-</b><br><b>management</b><br><b>{auto}]</b> | Provides additional media endpoint device TLVs to enable inventory and power management discovery. Specifies the LLDP MED TLVs to send or receive. <ul style="list-style-type: none"> <li>inventory-management – Enables inventory management discovery. Allows an endpoint to convey detailed inventory information about itself. This information includes details, such as manufacturer, model, and software version, etc. This option is enabled by default.</li> </ul> |
|                                                                                                                            | power-management auto – Enables extended power via MDI discovery. Allows endpoints to convey power information, such as how the device is powered, power priority, etc. <ul style="list-style-type: none"> <li>auto – Optional. Assigns default value based on device type</li> </ul>                                                                                                                                                                                       |

### Example

```

nx9500-6C8809(config-profile-default-rfs4000)#lldp timer 20

nx9500-6C8809(config-profile-default-rfs4000)#show context
profile rfs4000 default-rfs4000
bridge vlan 1
.....
use firewall-policy default
ip dns-server-forward
ip nat pool pool1
address range 172.16.10.2 172.16.10.8
ip nat inside source list test interface vlan1 pool pool1 overload
lldp timer 20
--More--
nx9500-6C8809(config-profile-default-rfs4000)#

```

### Related Commands

|                        |                               |
|------------------------|-------------------------------|
| <b>no</b> on page 1200 | Disables LLDP on this profile |
|------------------------|-------------------------------|

### load-balancing

[Profile Config Commands](#) on page 862

Configures load balancing parameters

#### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```

load-balancing [advanced-params | balance-ap-loads | balance-band-loads |
balance-channel-loads | band-control-startegy | band-ratio | group-id | neighbor-
selection-strategy]

```

```
load-balancing advanced-params [2.4GHz-load|5GHz-load|ap-load|equality-
margin| hiwater-threshold|max-neighbors|max-preferred-band-load|min-
common-clients|min-neighbor-rssi|min-probe-rssi]
```

```
load-balancing advanced-params [2.4GHz-load|5GHz-load|ap-load] [client-
weightage|throughput-weightage] <0-100>
```

```
load-balancing advanced-params equality-margin [2.4GHz|5GHz|ap|band]
<0-100>
```

```
load-balancing advanced-params hiwater-threshold [ap|channel-2.4GHz|
channel-5GHz]<0-100>
```

```
load-balancing advanced-params max-preferred-band-load [2.4GHz|5GHz]
<0-100>
```

```
load-balancing advanced-params [max-neighbors <0-16>|min-common-clients
<0-256>| min-neighbor-rssi <-100-30>|min-probe-rssi <-100-30>]
```

```
load-balancing [balance-ap-loads|balance-band-loads|balance-channel-loads
[2.4GHz|5GHz]]
```

```
load-balancing band-control-strategy [distribute-by-ratio|prefer-2.4GHz|
prefer-5GHz]
```

```
load-balancing band-ratio [2.4GHz|5GHz] [0|<1-10>]
```

```
load-balancing group-id <GROUP-ID>
```

```
load-balancing neighbor-selection-strategy [use-common-clients|use-roam-
notification|use-smart-rf]
```

### Parameters

```
load-balancing advanced-params [2.4GHz-load|5GHz-load|ap-load] [client-weightage|
throughput-weightage] <0-100>
```

|                                                                                                  |                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>load-balancing<br/>advanced-params</b>                                                        | Configures advanced load balancing parameters                                                                                                                                                        |
| <b>2.4GHz-load<br/>[client-<br/>weightage  <br/>throughput-<br/>weightage]<br/>&lt;0-100&gt;</b> | Configures 2.4 GHz load calculation weightages <ul style="list-style-type: none"><li>client-weightage - Specifies weightage assigned to the client-count when calculating the 2.4 GHz load</li></ul> |

|                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                              | <ul style="list-style-type: none"> <li>throughput-weightage – Specifies weightage assigned to throughput, when calculating the 2.4 GHz load</li> </ul> <p>The following keyword is common to the ‘client-weightage’ and ‘throughput-weightage’ parameters:</p> <ul style="list-style-type: none"> <li>&lt;0-100&gt; – Sets the margin as a load percentage from 1 - 100. The default client-weightage is 90%. The default throughput-weightage is 10%.</li> </ul>                                                                                                                                                                      |
| <b>5GHz-load</b><br><b>[client-weightage   throughput-weightage]</b><br><b>&lt;0-100&gt;</b> | <p>Configures 5.0 GHz load calculation weightages</p> <ul style="list-style-type: none"> <li>client-weightage – Specifies weightage assigned to the client-count when calculating the 5.0 GHz load</li> <li>throughput-weightage – Specifies weightage assigned to throughput, when calculating the 5.0 GHz load</li> </ul> <p>The following keyword is common to the ‘client-weightage’ and ‘throughput-weightage’ parameters:</p> <ul style="list-style-type: none"> <li>&lt;0-100&gt; – Sets the margin as a load percentage from 1 - 100. The default client-weightage is 90%. The default throughput-weightage is 10%.</li> </ul> |
| <b>ap-load</b><br><b>[client-weightage   throughput-weightage]</b><br><b>&lt;0-100&gt;</b>   | <p>Configures AP load calculation weightages</p> <ul style="list-style-type: none"> <li>client-weightage – Specifies weightage assigned to the client-count, when calculating the AP load</li> <li>throughput-weightage – Specifies weightage assigned to throughput, when calculating the AP load</li> </ul> <p>The following keyword is common to the ‘client-weightage’ and ‘throughput-weightage’ parameters:</p> <ul style="list-style-type: none"> <li>&lt;0-100&gt; – Sets the margin as a load percentage from 1 - 100. The default client-weightage is 90%. The default throughput-weightage is 10%.</li> </ul>               |

load-balancing advanced-params equality-margin [2.4GHz|5GHz|ap|band] <0-100>

|                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>load-balancing advanced-params</b>                                          | <p>Configures advanced load balancing parameters</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>equality-margin</b><br><b>[2.4GHz 5GHz ap band]</b><br><b>&lt;0-100&gt;</b> | <p>Configures the maximum load difference considered equal. The load is compared for different 2.4 GHz channels, 5.0 GHz channels, APs, or bands.</p> <ul style="list-style-type: none"> <li>2.4GHz – Configures the maximum load difference considered equal when comparing loads on different 2.4 GHz channels</li> <li>5GHz – Configures the maximum load difference considered equal when comparing loads on different 5.0 GHz channels</li> <li>ap – Configures the maximum load difference considered equal when comparing loads on different APs</li> <li>band – Configures the maximum load difference considered equal when comparing loads on different bands</li> </ul> <p>The following keyword is common to 2.4 GHz channels, 5.0 GHz channels, APs, and bands:</p> <ul style="list-style-type: none"> <li>&lt;0-100&gt; – Sets the margin as a load percentage from 1 - 100. The default equality-margin for 2.4 GHz, 5.0 GHz, ap, and band loads is 1%.</li> </ul> |

load-balancing advanced-params hiwater-threshold [ap|channel-2.4GHz|channel-5GHz] <0-100>

|                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>load-balancing advanced-params</b>                     | Configures advanced load balancing parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>hiwater-threshold</b>                                  | Configures the load beyond which load balancing is invoked                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>[ap   channel-2.4GHz   channel-5GHz] &lt;0-100&gt;</b> | <p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>ap - Configures the AP load beyond which load balancing begins</li> <li>channel-2.4GHz - Configures the AP load beyond which load balancing begins (for APs on 2.4 GHz channel)</li> <li>channel-5GHz - Configures the AP load beyond which load balancing begins for (APs on 5.0 GHz channel)</li> </ul> <p>The following keyword is common for the 'AP', 'channel-2.4GHz', and 'channel-5GHz' parameters:</p> <ul style="list-style-type: none"> <li>&lt;0-100&gt; - Sets the load threshold as a number from 1 - 100. The default hiwater-threshold for channel-2.5GHz, channel-5GHz, and ap loads is 5.</li> </ul> |

load-balancing advanced-params max-preferred-band-load [2.4GHz|5GHzd] <0-100>

|                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>load-balancing advanced-params</b> | Configures advanced load balancing parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>max-preferred-band-load</b>        | Configures the maximum load on the preferred band, beyond which the other band is equally preferred                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>[2.4GHz   5GHz] &lt;0-100&gt;</b>  | <p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>2.4GHz - Configures the maximum load on 2.4 GHz, when it is the preferred band</li> <li>5GHz - Configures the maximum load on 5.0 GHz, when it is the preferred band</li> </ul> <p>The following keyword is common to the 2.4 GHz and 5.0 GHz bands:</p> <ul style="list-style-type: none"> <li>&lt;0-100&gt; - Configures the maximum load as a percentage from 0 - 100. The default value for 2.4GHz and 5.0GHz is 75%.</li> </ul> |

load-balancing advanced-params [max-neighbors <0-16>|min-common-clients <0-256>|min-neighbor-rssi <-100-30>|min-probe-rssi <-100-30>]

|                                         |                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>load-balancing advanced-params</b>   | Configures advanced load balancing parameters                                                                                                                                                                                                                                                              |
| <b>max-neighbors &lt;0-16&gt;</b>       | <p>Configures the maximum number of confirmed neighbors to balance</p> <ul style="list-style-type: none"> <li>&lt;0-16&gt; - Specify a value from 0 - 16. Optionally configure a minimum of 0 neighbors and a maximum of 16 neighbors. The default is 16.</li> </ul>                                       |
| <b>min-common-clients &lt;0-256&gt;</b> | <p>Configures the minimum number of common clients that can be shared with the neighbor for load balancing</p> <ul style="list-style-type: none"> <li>&lt;0-256&gt; - Specify a value from 0 - 256. Optionally configure a minimum of 0 clients and a maximum of 256 clients. The default is 0.</li> </ul> |

|                                          |                                                                                                                                                                                                                                                                           |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>min-neighbor-rssi &lt;-100-30&gt;</b> | Configures the minimum signal strength (RSSI) of a neighbor detected <ul style="list-style-type: none"> <li>• &lt;-100-30&gt; – Sets the signal strength in dBm. Specify a value from -100 - 30 dBm. The default is -65 dBm.</li> </ul>                                   |
| <b>min-probe-rssi &lt;-100-30&gt;</b>    | Configures the minimum received probe signal strength required to qualify the sender as a common client <ul style="list-style-type: none"> <li>• &lt;0-100&gt; – Sets the signal strength in dBm. Specify a value from -100 - 30 dBm. The default is -100 dBm.</li> </ul> |

load-balancing [balance-ap-loads|balance-band-loads|balance-channel-loads [2.4GHz|5GHz]]

|                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>load-balancing</b>                      | Configures the following load balancing parameters: ap-loads, band-loads, and channel-loads.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>balance-ap-loads</b>                    | Enables neighbor AP load balancing. This option distributes the access point's radio load amongst other controller managed access point radios. This option is disabled by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>balance-band-loads</b>                  | Enables balancing of the total band load amongst neighbors. This option balances the access point's radio load by assigning a ratio to both the 2.4 GHz and 5.0 GHz bands. Balancing radio load by band ratio allows an administrator to assign a greater weight to radio traffic on either the 2.4 GHz or 5.0 GHz band. This option is disabled by default.                                                                                                                                                                                                                                                                                        |
| <b>balance-channel-loads [2.4GHz 5GHz]</b> | Enables the following: <ul style="list-style-type: none"> <li>• 2.4GHz – Channel load balancing on 2.4 GHz band. This option is disabled by default. Balances the access point's 2.4 GHz radio load across channels supported within the country of deployment. This can prevent congestion on the 2.4 GHz radio if a channel is over utilized.</li> <li>• 5GHz – Channel load balancing on 5.0 GHz band. This option is disabled by default. Balances the access point's 5.0 GHz radio load across channels supported within the country of deployment. This can prevent congestion on the 5.0 GHz radio if a channel is over utilized.</li> </ul> |

load-balancing band-control-strategy [distribute-by-ratio|prefer-2.4GHz|prefer-5GHz]

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>load-balancing band-control-strategy</b> | Configures a band control strategy<br>By default, this option steers 5.0 GHz-capable clients to the 5.0 GHz band. When an access point hears a request from a client to associate on both the 2.4 GHz and 5.0 GHz bands, it knows the client is capable of operation in 5.0 GHz. Band steering steers the client by responding only to the 5.0 GHz association request and not the 2.4 GHz request. Consequently, the client only associates in the 5.0 GHz band. |
| <b>distribute-by-ratio</b>                  | Distributes clients to either band according to the band-ratio                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>prefer-2.4GHz</b>                        | Nudges all dual-band clients to 2.4 GHz band                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>prefer-5GHz</b>                          | Nudges all dual-band clients to 5.0 GHz band. This is the default setting.                                                                                                                                                                                                                                                                                                                                                                                        |

load-balancing band-ratio [2.4GHz|5GHz] [0|<1-10>]

|                                  |                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>load-balancing band-ratio</b> | Configures the relative loading of 2.4 GHz band and 5.0 GHz band. This allows an administrator to weight client traffic load if wishing to prioritize client traffic load on the 2.4 GHz or the radio band. The higher the value set, the greater the weight assigned to radio traffic load on the 2.4 GHz or 5.0 GHz radio band. |
| <b>2.4GHz [0   &lt;1-10&gt;]</b> | Configures the relative loading of 2.4 GHz band <ul style="list-style-type: none"> <li>• 0 - Selecting '0' steers all dual-band clients preferentially to the other band</li> <li>• &lt;0-10&gt; - Configures a relative load as a number from 0 - 10. The default is 0.</li> </ul>                                               |
| <b>5ghz [0   &lt;1-10&gt;]</b>   | Configures the relative loading of 5.0 GHz band <ul style="list-style-type: none"> <li>• 0 - Selecting '0' steers all dual-band clients preferentially to the other band</li> <li>• &lt;0-10&gt; - Configures a relative load as a number from 0 - 10. The default is 1.</li> </ul>                                               |

load-balancing group-id <GROUP-ID>

|                                                 |                                                                                                                                                                                                          |
|-------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>load-balancing group-id &lt;GROUP-ID&gt;</b> | Configures group ID to facilitate load balancing <ul style="list-style-type: none"> <li>• &lt;GROUP-ID&gt; - Specify the group ID. This option is enabled only when a group ID is configured.</li> </ul> |
|-------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

load-balancing neighbor-selection-strategy [use-common-clients|use-roam-notification|use-smart-rf]

|                                                   |                                                                                                                        |
|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| <b>load-balancing neighbor-selection-strategy</b> | Configures a neighbor selection strategy. The options are: use-common-clients, use-roam-notification, and use-smart-rf |
| <b>use-common-clients</b>                         | Selects neighbors based on probes from clients common to neighbors. This option is enabled by default.                 |
| <b>use-roam-notification</b>                      | Selects neighbors based on roam notifications from roamed clients. This option is enabled by default.                  |
| <b>use-smart-rf</b>                               | Selects neighbors detected by Smart RF. This option is enabled by default.                                             |

### Example

```
nx9500-6C8809(config-profile-default-rfs4000)#load-balancing advanced-params 2.4ghz-load throughput-weightage 90
```

```
nx9500-6C8809(config-profile-default-rfs4000)#load-balancing advanced-params hiwater-threshold ap 90
```

```
nx9500-6C8809(config-profile-default-rfs4000)#load-balancing balance-ap-loads
```

```
rfs7000-37FABE(config-profile-default-rfs4000)#show context
profile rfs4000 default-rfs4000
bridge vlan 1
bridging-mode isolated-tunnel
ip igmp snooping
ip igmp snooping querier
ip default-gateway 172.16.10.4
autoinstall configuration
autoinstall firmware
load-balancing advanced-params 2.4ghz-load throughput-weightage 90
load-balancing advanced-params hiwater-threshold ap 90
load-balancing balance-ap-loads
--More--
nx9500-6C8809(config-profile-default-rfs4000)#
```

## Related Commands

|                              |                                         |
|------------------------------|-----------------------------------------|
| <code>no</code> on page 1200 | Disables load balancing on this profile |
|------------------------------|-----------------------------------------|

### *logging*

[Profile Config Commands](#) on page 862

Enables message logging and configures logging settings. When enabled, the profile logs individual system events to a user-defined log file or a syslog server. Message logging is disabled by default.

Enabling message logging is recommended, because system event logs can be analyzed to determine an overall pattern that may be negatively impacting performance.

This command can also be executed in the device configuration mode.

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
logging [aggregation-time | buffered | console | facility | forward | host | on |
syslog]
```

```
logging [aggregation-time <1-60> | host [<IPv4> | <IPv6>] {port <1-65535>} |
on]
```

```
logging [buffered | console | syslog | forward] [<0-7> | emergencies | alerts |
critical | errors | warnings | notifications | informational | debugging]
```

```
logging facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 |
local7]
```

### Parameters

```
logging [aggregation-time <1-60> | host [<IPv4> | <IPv6>] {port <1-65535>} | on]
```

|                                      |                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>logging</b>                       | Enables message logging and configures logging settings                                                                                                                                                                                                                                                                                 |
| <b>aggregation-time &lt;1-60&gt;</b> | Sets the number of seconds for aggregating repeated messages. This is the interval at which system events are logged on behalf of this profile. The shorter the interval, the sooner the event is logged. <ul style="list-style-type: none"><li>• &lt;1-60&gt; - Specify a value from 1 - 60 seconds. The default value is 0.</li></ul> |



|                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>host</b> [<IPv4>   <IPv6>] {port <1-65535>} | Configures a remote host to receive log messages. Defines numerical (non DNS) IPv4 or IPv6 addresses for external resources where logged system events can be sent on behalf of the profile (or device). A maximum of four entries can be made. <ul style="list-style-type: none"> <li>• &lt;IPv4&gt; - Specify the IPv4 address of the remote host.</li> <li>• &lt;IPv6&gt; - Specify the IPv6 address of the remote host.</li> <li>• port &lt;1-65535&gt; - Optional. Configures the syslog port</li> <li>• &lt;1-65535&gt; - Specify the syslog port from 1 - 65535. The default port is 514.</li> </ul> |
| <b>on</b>                                      | Enables the logging of system messages                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

logging [buffered|console|syslog|forward] [<0-7>|emergencies|alerts|critical| errors| warnings|notifications|informational|debugging]

|                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>logging</b>                                                                                            | Enables message logging and configures logging settings                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>buffered</b>                                                                                           | Sets the buffered logging level                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>console</b>                                                                                            | Sets the console logging level                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>syslog</b>                                                                                             | Sets the syslog server's logging level                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>forward</b>                                                                                            | Forwards system debug messages to the wireless controller or service platform                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| [<0-7>   alerts   critical   debugging   emergencies   errors   informational   notifications   warnings] | <p>The following keywords are common to the buffered, console, syslog, and forward parameters.</p> <p>All incoming messages have different severity levels based on their importance. The severity level is fixed on a scale of 0 - 7.</p> <ul style="list-style-type: none"> <li>• &lt;0-7&gt; - Sets the message logging severity level on a scale of 0 - 7</li> <li>• emergencies - Severity level 0: System is unusable</li> <li>• alerts - Severity level 1: Requires immediate action</li> <li>• critical - Severity level 2: Critical conditions</li> <li>• errors - Severity level 3: Error conditions</li> <li>• warnings - Severity level 4: Warning conditions (default)</li> <li>• notifications - Severity level 5: Normal but significant conditions</li> <li>• informational - Severity level 6: Informational messages</li> <li>• debugging - Severity level 7: Debugging messages</li> </ul> |

logging facility [local0|local1|local2|local3|local4|local5|local6|local7]

|                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>logging</b>                                                                          | Enables message logging and configures logging settings                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>facility</b> [local0   local1   local2   local3   local4   local5   local6   local7] | <p>Enables the syslog to decide where to send the incoming message</p> <p>There are 8 logging facilities, from syslog0 to syslog7.</p> <ul style="list-style-type: none"> <li>• local0 - Syslog facility local0</li> <li>• local1 - Syslog facility local1</li> <li>• local2 - Syslog facility local2</li> <li>• local3 - Syslog facility local3</li> <li>• local4 - Syslog facility local4</li> <li>• local5 - Syslog facility local5</li> <li>• local6 - Syslog facility local6</li> <li>• local7 - Syslog facility local7</li> </ul> |

## Example

```
NOC-NX9500(config-profile-testNX9000)#logging facility local4

NOC-NX9500(config-profile-testNX9000)#show context include-factory | include logging
no logging on
logging aggregation-time 0
logging console warnings
logging buffered warnings
logging syslog warnings
logging facility local4
logging forward errors
no l2tpv3 logging
no dpi logging on
dpi logging level notifications
NOC-NX9500(config-profile-testNX9000)#
```

## Related Commands

|                              |                                  |
|------------------------------|----------------------------------|
| <code>no</code> on page 1200 | Disables logging on this profile |
|------------------------------|----------------------------------|

## *mac-address-table*

[Profile Config Commands](#) on page 862

Configures the MAC address table. Use this command to create MAC address table entries by assigning a static address to the MAC address table.

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
mac-address-table [aging-time|detect-gateways|static]
mac-address-table aging-time [0|<10-1000000>]
mac-address-table detect-gateways
mac-address-table static <MAC> vlan <1-4094> interface [<L2-INTERFACE>|ge
<1-4>| port-channel <1-2>]
```

### Parameters

```
mac-address-table aging-time [0|<10-1000000>]
```

|                                                            |                                                                                                                                                                                                                                                                                     |
|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mac-address-table aging-time [0 &lt;10-1000000&gt;]</b> | Sets the duration a learned MAC address persists after the last update <ul style="list-style-type: none"><li>• 0 - Entering the value '0' disables the aging time</li><li>• &lt;10-1000000&gt; - Sets the aging time from 10 -100000 seconds. The default is 300 seconds.</li></ul> |
|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
mac-address-table detect-gateways
```

|                                          |                                                                                                     |
|------------------------------------------|-----------------------------------------------------------------------------------------------------|
| <b>mac-address-table detect-gateways</b> | Enables automatic detection of gateways. Detected gateways are remembered in the MAC address table. |
|------------------------------------------|-----------------------------------------------------------------------------------------------------|

```
mac-address-table static <MAC> vlan <1-4094> interface [<L2-INTERFACE>|ge <1-4>| port-channel <1-2>]
```

|                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mac-address-table static &lt;MAC&gt;</b>                                       | Creates a static MAC address table entry <ul style="list-style-type: none"> <li>&lt;MAC&gt; - Specifies the static address to add to the MAC address table. Specify the MAC address in the AA-BB-CC-DD-EE-FF, AA:BB:CC:DD:EE:FF, or AABB.CCDD.EEFF format.</li> </ul>                                                                                                                                                                                                                                                                                                                                |
| <b>vlan &lt;1-4094&gt;</b>                                                        | Assigns a static MAC address to a specified VLAN port <ul style="list-style-type: none"> <li>&lt;1-4094&gt; - Specify the VLAN index from 1 - 4094.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>interface [&lt;L2-INTERFACE&gt;  ge &lt;1-4&gt;  port-channel &lt;1-2&gt;]</b> | Specifies the interface type. The options are: layer 2 Interface, GigabitEthernet interface, and a port channel interface <ul style="list-style-type: none"> <li>&lt;L2-INTERFACE&gt; - Specify the layer 2 interface name.</li> <li>ge - Specifies a GigabitEthernet interface <ul style="list-style-type: none"> <li>&lt;1-4&gt; - Specify the GigabitEthernet interface index from 1 - 4.</li> </ul> </li> <li>port-channel - Specifies a port channel interface <ul style="list-style-type: none"> <li>&lt;1-2&gt; - Specify the port channel interface index from 1 - 2.</li> </ul> </li> </ul> |

### Example

```
nx9500-6C8809(config-profile-default-rfs4000)#mac-address-table static 00-40-96-B0-BA-2A
vlan 1 interface ge 1
```

```
nx9500-6C8809(config-profile-default-rfs4000)#show context
profile rfs4000 default-rfs4000
 bridge vlan 1

 logging facility local4
 mac-address-table static 00-40-96-B0-BA-2A vlan 1 interface ge1
 ip nat pool pool1
 --More--
nx9500-6C8809(config-profile-default-rfs4000)#
```

### Related Commands

|                        |                                               |
|------------------------|-----------------------------------------------|
| <b>no</b> on page 1200 | Disables or reverts settings to their default |
|------------------------|-----------------------------------------------|

### mac-auth

[Profile Config Commands](#) on page 862

Enables authentication of a client's MAC address on wired ports. When configured, MAC authentication will be enabled on devices using this profile.

To enable MAC address authentication on a device, enter the device's configuration mode and execute the mac-auth command.

When enabled, the source MAC address of a device, connected to the specified wired port, is authenticated with the RADIUS server. Once authenticated the device is permitted access to the managed network and packets from the authenticated source are processed. If not authenticated the

device is either denied access or provided guest access through the guest VLAN (provided guest VLAN access is configured on the port).

Enabling MAC authentication requires you to first configure a AAA policy specifying the RADIUS server. Configure the client's MAC address on the specified RADIUS server. Attach this AAA policy to a profile or a device. Finally, enable MAC authentication on the desired wired port of the device or device-profile.

Only one MAC address is supported for every wired port. Consequently, when one source MAC address is authenticated, packets from all other sources are dropped.

To enable client MAC authentication on a wired port:

- 1 Configure the user on the RADIUS server. The following examples create a RADIUS server user entry.

```
<DEVICE>(config)#radius-group <RAD-GROUP-NAME>
<DEVICE>(config-radius-group-<RAD-GROUP-NAME>)#policy vlan <VLAN-ID>

<DEVICE>(config)#radius-user-pool-policy <RAD-USER-POOL-NAME>
<DEVICE>(config-radius-user-pool-<RAD-USER-POOL-NAME>)#user <USER-NAME> password
<PASSWORD> group <RAD-GROUP-OF-STEP-A>
```

Note: The <USER-NAME> and <PASSWORD> should be the client's MAC address. This address will be matched against the MAC address of incoming traffic at the specified wired port.

```
<DEVICE>(config)#radius-server-policy <RAD-SERVER-POL-NAME>
<DEVICE>(config-radius-server-policy-<RAD-SERVER-POL-NAME>)#use radius-user-pool-policy
<RAD-USER-POOL-OF-STEP-B>
```

- 2 Configure a AAA policy exclusively for wired MAC authentication and specify the authentication (RADIUS) server settings. The following example creates a AAA policy 'macauth' and enters its configuration mode:

```
<DEVICE-A>(config)#aaa-policy macauth
<DEVICE-A>(config-aaa-policy-macauth)#...
```

Specify the RADIUS server details.

```
<DEVICE-A>(config)#aaa-policy macauth
<DEVICE-A>(config-aaa-policy-macauth)#authentication server <1-6> [host <IP>|onboard]
```

- 3 Attach the AAA policy to the device or profile. When attached to a profile, the AAA policy is applied to all devices using this profile.

```
<DEVICE>(config-device-aa-bb-cc-dd-ee)#mac-auth use aaa-policy macauth
<DEVICE>(config-profile-<DEVICE-PROFILE-NAME>)#mac-auth use aaa-policy macauth
```

- 4 Enable mac-auth on the device's desired GE port. When enabled on a profile, MAC address authentication is enabled, on the specified GE port, of all devices using this profile.

```
<DEVICE>(config-device-aa-bb-cc-dd-ee)#interface ge x
<DEVICE>(config-device-aa-bb-cc-dd-ee-gex)#mac-auth
```

```
<DEVICE>(config-profile-<PROFILE-NAME>)#interface ge x
<DEVICE>(config-profile-<PROFILE-NAME>)#mac-auth
```

#### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000

- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

## Syntax

```
mac-auth use aaa-policy <AAA-POLICY-NAME>
```

## Parameters

```
mac-auth use aaa-policy <AAA-POLICY-NAME>
```

|                                               |                                                                                                                                                                                           |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mac-auth</b>                               | Enables 802.1X authentication of MAC addresses on this profile. Use the device configuration mode to enable this feature on a device.                                                     |
| <b>use aaa-policy &lt;AAA-POLICY-NAME&gt;</b> | Associates an existing AAA policy with this profile (or device) <AAA-POLICY NAME> - Specify the AAA policy name. The AAA policy used should be created especially for MAC authentication. |

## Example

The following examples demonstrate the configuration of authentication of MAC addresses on wired ports:

```
rfs4000-229D58(config-aaa-policy-mac-auth)#authentication server 1 onboard controller
```

```
rfs4000-229D58(config-aaa-policy-mac-auth)#show context
aaa-policy mac-auth
 authentication server 1 onboard controller
rfs4000-229D58(config-aaa-policy-mac-auth)#
```

```
rfs4000-229D58(config)#radius-group RG
rfs4000-229D58(config-radius-group-RG)#policy vlan 11
```

```
rfs4000-229D58(config-radius-group-RG)#show context
radius-group RF
 policy vlan 11
rfs4000-229D58(config-radius-group-RG)#
```

```
rfs4000-229D58(config)#radius-user-pool-policy RUG
rfs4000-229D58(config-radius-user-pool-RUG)#user 00-16-41-55-F8-5D password 0
0-16-41-55-F8-5D group RG
```

```
rfs4000-229D58(config-radius-user-pool-RUG)#show context
radius-user-pool-policy RUG
 user 00-16-41-55-F8-5D password 0 00-16-41-55-F8-5D group RG
rfs4000-229D58(config-radius-user-pool-RUG)#
```

```
rfs4000-229D58(config)#radius-server-policy RS
rfs4000-229D58(config-radius-server-policy-RS)#use radius-user-pool-policy RUG
```

```
rfs4000-229D58(config-radius-server-policy-RS)#show context
radius-server-policy RS
 use radius-user-pool-policy RUG
rfs4000-229D58(config-radius-server-policy-RS)#
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-if-ge4)#show context
interface ge4
 dot1x authenticator host-mode single-host
 dot1x authenticator port-control auto
 mac-auth
rfs4000-229D58(config-device-00-23-68-22-9D-58-if-ge4)#
```

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-if-ge5)#show context
```

```

interface ge5
 switchport mode access
 switchport access vlan 1
 dot1x authenticator host-mode single-host
 dot1x authenticator guest-vlan 5
 dot1x authenticator port-control auto
 mac-auth
rfs4000-229D58(config-device-00-23-68-22-9D-58-if-ge5)#

rfs4000-229D58(config-device-00-23-68-22-9D-58)#show macauth interface ge 4
Mac Auth info for interface GE4

Mac Auth Enabled
Mac Auth Authorized Client MAC 00-16-41-55-F8-5D

rfs4000-229D58(config-device-00-23-68-22-9D-58)#

rfs4000-229D58(config-device-00-23-68-22-9D-58)#show macauth interface ge 5
Mac Auth info for interface GE5

Mac Auth Enabled
Mac Auth Not Authorized

rfs4000-229D58(config-device-00-23-68-22-9D-58)#

```

### Related Commands

|                        |                                                                                              |
|------------------------|----------------------------------------------------------------------------------------------|
| <b>no</b> on page 1200 | Disables authentication of MAC addresses on wired ports settings on this profile (or device) |
|------------------------|----------------------------------------------------------------------------------------------|

### *management-server*

[Profile Config Commands](#) on page 862

Configures a management server with this profile. This command is also applicable to the device configuration context.

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
management-server <HOST-NAME> port <1-65535>
```

### Parameters

```
management-server <HOST-NAME> port <1-65535>
```

**management-server** <HOST-NAME> port <1-65535>

Configures a management server with this profile. Use this command to identify the management server.

- <HOST-NAME> - Specify the management server's host name.
- port <1-65535> - Specify the port where the management server is reachable. The default setting is port 443.

**Note:** If the adoption-mode, on this profile, is set to 'cloud', ensure that the management-server configuration points to the ExtremeCloud Web address. If the adoption-mode is set to 'ws-controller', provide the ESE controller's IP address or hostname as the management server. For information on configuring the adoption-mode, see [adoption-mode](#) on page 868.

### Example

```
nx9500-6C8809(config-profile-testRFS4000)#management-server nx9500-6C8809 port 300

nx9500-6C8809(config-profile-testRFS4000)#show context include-factory | include
management-server
 management-server nx9500-6C8809 port 300
nx9500-6C8809(config-profile-testRFS4000)#
```

### Related Commands

|                                 |                                             |
|---------------------------------|---------------------------------------------|
| <a href="#">no</a> on page 1200 | Removes the management server configuration |
|---------------------------------|---------------------------------------------|

### *meshpoint-device*

[Profile Config Commands](#) on page 862

Configures meshpoint device parameters. This feature is configurable in the profile and device configuration modes.

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
meshpoint-device <MESHPOINT-NAME>
```

### Parameters

```
meshpoint-device <MESHPOINT-NAME>
```

**meshpoint-device** <MESHPOINT-NAME>

Configures meshpoint device parameters

- <MESHPOINT-NAME> - Specify meshpoint name.

## Usage Guidelines

For VMM (Vehicular Mounted Modem) access points or other mobile devices, set the path selection method as mobile-snr-leaf in the config-meshpoint-device mode. For more information, see [path-method \(meshpoint-device-config\)](#) on page 1796.

```
nx9500-6C8809(config-profile-testAP7161)#meshpoint-device test

nx9500-6C8809(config-profile-testAP7161-meshpoint-test)#?
Mesh Point Device Mode commands:
 acs Configure auto channel selection parameters
 exclude Exclude neighboring Mesh Devices
 hysteresis Configure path selection SNR hysteresis values
 monitor Event Monitoring
 no Negate a command or set its defaults
 path-method Path selection method used to find a root node
 preferred Configure preferred path parameters
 root Set this meshpoint as root
 root-select Root selection method parameters

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-profile-testAP7161-meshpoint-test)#
```

## Related Commands

|                                 |                               |
|---------------------------------|-------------------------------|
| <a href="#">no</a> on page 1200 | Removes a specified meshpoint |
|---------------------------------|-------------------------------|



### Note

For more information on the meshpoint-device configuration parameters, see [MESHPOINT](#) on page 1760.

### *meshpoint-monitor-interval*

[Profile Config Commands](#) on page 862

Configures the meshpoint monitoring interval. This is the interval, in seconds, at which the meshpoint status is checked.

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000



## Syntax

```
meshpoint-monitor-interval <1-65535>
```

## Parameters

```
meshpoint-monitor-interval <1-65535>
```

|                                                             |                                                                                                                                                                                                     |
|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>meshpoint-monitor-interval</b><br><b>&lt;1-65535&gt;</b> | Configures the meshpoint monitoring interval in seconds <ul style="list-style-type: none"><li>• &lt;1-65535&gt; - Specify the interval from 1 - 65535 seconds. The default is 30 seconds.</li></ul> |
|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Example

```
nx9500-6C8809(config-profile-default-rfs4000)#meshpoint-monitor-interval 100

nx9500-6C8809(config-profile-default-rfs4000)#show context
profile rfs4000 default-rfs4000
 bridge vlan 1
 bridging-mode isolated-tunnel
 ip igmp snooping
 ip igmp snooping querier
 meshpoint-monitor-interval 100
 ip default-gateway 172.16.10.4
 --More--
nx9500-6C8809(config-profile-default-rfs4000)#
```

## Related Commands

|                                 |                                                                  |
|---------------------------------|------------------------------------------------------------------|
| <a href="#">no</a> on page 1200 | Resets the meshpoint monitoring interval to default (30 seconds) |
|---------------------------------|------------------------------------------------------------------|

### *min-misconfiguration-recovery-time*

[Profile Config Commands](#) on page 862

Configures the minimum device connectivity verification time

#### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

## Syntax

```
min-misconfiguration-recovery-time <60-3600>
```

## Parameters

```
min-misconfiguration-recovery-time <60-3600>
```

|                                                                     |                                                                                                                                                                                                                            |
|---------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>min-misconfiguration-recovery-time</b><br><b>&lt;60-3600&gt;</b> | Configures the minimum connectivity (with the associated device) verification interval <ul style="list-style-type: none"><li>• &lt;60-3600&gt; - Specify a value from 60 - 3600 seconds (default is 60 seconds).</li></ul> |
|---------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Example

```
NOC-NX9500(config-profile-testNX9000)#min-misconfiguration-recovery-time 500

NOC-NX9500(config-profile-testNX9000)#show context include-factory | include min-
-misconfiguration-recovery-time
 min-misconfiguration-recovery-time 500
NOC-NX9500(config-profile-testNX9000)#
```

## Related Commands

|                              |                                        |
|------------------------------|----------------------------------------|
| <code>no</code> on page 1200 | Resets setting to default (60 seconds) |
|------------------------------|----------------------------------------|

*mint*

[Profile Config Commands](#) on page 862

Configures MiNT protocol parameters required for MiNT creation and adoption

MiNT links are required for adoption of a device (APs, wireless controller, and service platform) to a controller. The MiNT link is created on both the adoptee and the adopter. WiNG provides several commands to configure MiNT links and establish adoption for both IPv4 and IPv6 addresses.

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
mint [dis|inter-tunnel-bridging|level|link|mlcp|rate-limit|spf-latency|
tunnel-across-extended-vlan|tunnel-controller-load-balancing]
```

```
mint dis [priority-adjustment <-255-255>|strict-evis-reachability]
```

```
mint inter-tunnel-bridging
```

```
mint level 1 area-id [<1-16777215>|<NUMBER-ALIAS-NAME>]
```

```
mint link [force|ip|listen|vlan]
```

```
mint link force ip [<IPv4>|<IPv6>] [<1-65535> level 2|level 2]
{adjacency-hold-time <2-600>|cost <1-10000>|hello-interval <1-120>|ipsec-
secure {gw [<IP>|<HOST-NAME>]}}
```

```
mint link [listen ip [<IPv4>|<IPv6>|<HOST-ALIAS-NAME>]|vlan <1-4094>]
{adjacency-hold-time <2-600>|cost <1-10000>|hello-interval <1-120>|ipsec-
security {gw [<IP>|<HOST-NAME>]}}|level [1|2]}
```

```
mint link ip [<IPv4>|<IPv6>|<HOST-ALIAS-NAME>] {<1-65535>/adjacency-hold-
time <2-600>/cost <1-10000>/hello-interval <1-120>/ipsec-security {gw
[<IP>|<HOST-NAME>]}/level [1/2]}
```

```
mint mlcp [ip|ipv6|vlan]
```

```
mint rate-limit level2 [link|mlcp]
```

```
mint rate-limit level2 [link [ip [<IPv4>|<IPv6>] <1-65535>|vlan
<1-4094>]|mlcp [ip|ipv6|vlan]] rate <50-1000000> max-burst-size <2-1024>
{red-threshold [background|best-effort|video|voice] <0-100>}
```

```
mint spf-latency <0-60>
```

```
mint tunnel-across-extended-vlan
```

```
mint tunnel-controller-load-balancing level1
```

### Parameters

```
mint dis [priority-adjustment <-255-255>|strict-evis-reachability]
```

|                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mint</b>                                     | Configures MiNT protocol parameters required for MiNT link creation and adoption                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>dis priority-adjustment &lt;-255-255&gt;</b> | <p>Sets the relative priority for the router to become DIS (designated router)</p> <ul style="list-style-type: none"> <li>priority-adjustment - Sets priority adjustment added to base priority</li> </ul> <p>The Designated IS (DIS) priority adjustment is the value added to the base level DIS priority to influence the DIS election. A value of +1 or greater increases DISiness.</p> <ul style="list-style-type: none"> <li>&lt;-255-255&gt; - Specify a value from -255 - 255. The default is 0.</li> </ul> <p>Higher numbers result in higher priorities</p> |
| <b>strict-evis-reachability</b>                 | Enables reaching Ethernet Virtualization Interconnect (EVIS) election winners through MiNT. This option is enabled by default.                                                                                                                                                                                                                                                                                                                                                                                                                                        |

```
mint inter-tunnel-bridging
```

|                              |                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mint</b>                  | Configures MiNT protocol parameters required for MiNT link creation, adoption and communication                                                                                                                                                                                                                                                                                                            |
| <b>inter-tunnel-bridging</b> | Enables forwarding of broadcast multicast (BCMC) packets between devices communicating via Level 2 MiNT links. When enabled, MiNT tunnels across Level 2, adopted access points are bridged. One of the advantages of inter-tunnel bridging is the enabling of roaming between these access points. This option is disabled by default. If enabling this option, use ACLs to filter unwanted BCMC traffic. |

```
mint level 1 area-id [<1-16777215>|<NUMBER-ALIAS-NAME>]
```

|                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mint</b>                                                   | Configures MiNT protocol parameters required for MiNT link creation and adoption                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>level 1</b>                                                | Configures local MiNT routing settings <ul style="list-style-type: none"> <li>1 - Configures local MiNT routing level</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>area-id</b><br>[<1-16777215>  <br><NUMBER-ALIAS-<br>NAME>] | Specifies the level 1 routing area identifier. Use one of the following options to specify the area ID: <ul style="list-style-type: none"> <li>&lt;1-16777215&gt; - Specify a value from 1 - 16777215.</li> <li>&lt;NUMBER-ALIAS-NAME&gt; - Specify a number alias (should be existing and configured). Aliases are configuration items that can be defined once and used in different configuration contexts. For more information on creating a number alias, see <a href="#">alias</a> on page 237.</li> </ul> |

```
mint link force ip [<IPv4>|<IPv6>] [<1-65535> level 2|level 2] {adjacency-hold-time
<2-600>|cost <1-10000>|hello-interval <1-120>|ipsec-security {gw [<IP>|<HOST-NAME>]}}
```

|                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mint</b>                                          | Configures MiNT protocol parameters required for MiNT link creation and adoption                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>link force</b>                                    | Creates a MiNT routing link as a forced link <ul style="list-style-type: none"> <li>force - Forces a MiNT routing link to be created even if not necessary</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>ip</b> [<IPv4>  <br><IPv6>]                       | Creates a MiNT tunnel over UDP/IPv4 or IPv6<br>Use this keyword to specify the IP address (IPv4 or IPv6) used by peers for inter-operation when supporting the MiNT protocol. <ul style="list-style-type: none"> <li>&lt;IPv4&gt; - Specify the MiNT tunnel peer's IPv4 address.</li> <li>&lt;IPv6&gt; - Specify the MiNT tunnel peer's IPv6 address.</li> </ul> <p>After specifying the MiNT peer's address, configure the following MiNT link parameters: UDP port, adjacency-hold-time, cost, hello-interval, IPSec security gateway, and routing level.</p> |
| <b>&lt;1-65535&gt; level 2</b>                       | Optional. Specifies a custom UDP port for MiNT links. Specify the port from 1 - 65535. <ul style="list-style-type: none"> <li>level - Specifies the routing level <ul style="list-style-type: none"> <li>2 - Configures level 2 inter-site MiNT routing</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                  |
| <b>adjacency-hold-time &lt;2-600&gt;</b>             | Optional. Specifies the adjacency lifetime after hello packets cease <ul style="list-style-type: none"> <li>&lt;2-600&gt; - Specify a value from 2 - 600 seconds. The default is 46 seconds.</li> </ul>                                                                                                                                                                                                                                                                                                                                                         |
| <b>cost &lt;1-100000&gt;</b>                         | Optional. Specifies the link cost in arbitrary units <ul style="list-style-type: none"> <li>&lt;1-100000&gt; - Specify a value from 1 - 100000. The default is 100.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>hello-interval &lt;1-120&gt;</b>                  | Optional. Specifies the interval, in seconds, between successive hello packets <ul style="list-style-type: none"> <li>&lt;1-120&gt; - Specify a value from 1 - 120 seconds. The default is 15 seconds.</li> </ul>                                                                                                                                                                                                                                                                                                                                               |
| <b>ipsec-security</b><br>{gw [<IP> <br><HOST-NAME>]} | Optional. Enables IPSec secure peer authentication on the MiNT link connection (link). This option is disabled by default. <ul style="list-style-type: none"> <li>gw [&lt;IP&gt; &lt;HOSTNAME&gt;] - Optional. Configures the IPSec secure gateway. When enabling IPSec, you can optionally specify the IPSec secure gateway's numerical IP address or administrator defined hostname.</li> </ul>                                                                                                                                                               |

```
mint link [listen ip [<IPv4>|<IPv6>|<HOST-ALIAS-NAME>]|vlan <1-4094>] {adjacency-hold-time
<2-600>|cost <1-10000>|hello-interval <1-120>|level [1|2]|ipsec-security {gw [<IP>|<HOST-
NAME>]}}
```

|                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mint</b>                                                        | Configures MiNT protocol parameters required for MiNT link creation and adoption                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>link listen ip</b><br>[<IPv4> <IPv6> <br><HOST-ALIAS-<br>NAME>] | <p>Creates a MiNT routing link</p> <ul style="list-style-type: none"> <li>listen – Creates a MiNT listening link</li> <li>ip – Creates a MiNT listening link over UDP/IP or IPv6 <ul style="list-style-type: none"> <li>&lt;IPv4&gt; – Specify the IPv4 address of the listening UDP/IP link.</li> <li>&lt;IPv6&gt; – Specify the IPv6 address of the listening UDP/IP link.</li> <li>&lt;HOST-ALIAS-NAME&gt; – Specify the host alias identifying the MiNT link address. The host alias should existing and configured.</li> </ul> </li> </ul> <p>UDP/IP links can be created by configuring a matching pair of links, one on each end point. However, that is error prone and does not scale. So UDP/IP links can also listen (in the TCP sense), and dynamically create connected UDP/IP links when contacted. The typical configuration is to have a listening UDP/IP link on the IP address S.S.S.S, and for all the APs to have a regular UDP/IP link to S.S.S.S.</p> |
| <b>link vlan</b><br><1-4094>                                       | <p>Enables MiNT routing on VLAN</p> <ul style="list-style-type: none"> <li>vlan – Defines a VLAN ID used by peers for inter-operation when supporting the MiNT protocol.</li> <li>&lt;1-4094&gt; – Select VLAN ID from 1 - 4094.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>adjacency-hold-time</b> <2-600>                                 | <p>This parameter is common to the 'listen' and 'vlan' parameters:</p> <ul style="list-style-type: none"> <li>adjacency-hold-time &lt;2-600&gt; – Optional. Specifies the adjacency lifetime after hello packets cease</li> <li>&lt;2-600&gt; – Specify a value from 2 - 600 seconds. The default is 46 seconds.</li> </ul> <p>For MiNT VLAN routing, the default is 13 seconds.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>cost</b> <1-100000>                                             | <p>This parameter is common to the 'listen' and 'vlan' parameters:</p> <ul style="list-style-type: none"> <li>cost &lt;1-100000&gt; – Optional. Specifies the link cost in arbitrary units</li> <li>&lt;1-100000&gt; – Specify a value from 1 - 100000. The default is 100.</li> </ul> <p>For MiNT VLAN routing, the default is 10.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>hello-interval</b><br><1-120>                                   | <p>This parameter is common to the 'listen' and 'vlan' parameters:</p> <ul style="list-style-type: none"> <li>hello-interval &lt;1-120&gt; – Optional. Specifies the interval, in seconds, between successive hello packets</li> <li>&lt;1-120&gt; – Specify a value from 1 - 120. The default is 15 seconds.</li> </ul> <p>For MiNT VLAN routing the default is 4 seconds.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>level</b> [1 2]                                                 | <p>This parameter is common to the 'listen' and 'vlan' parameters:</p> <p>Optional. Specifies the routing levels for this routing link. The options are:</p> <ul style="list-style-type: none"> <li>1 – Configures local routing</li> <li>2 – Configures inter-site routing</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>ipsec-security</b><br>{gw [<IP> <br><HOST-NAME>]}               | <p>This parameter is common to the 'listen' and 'vlan' parameters:</p> <ul style="list-style-type: none"> <li>ipsec-security – Optional. Enables IPSec secure peer authentication on the MiNT connection (link). This option is disabled by default.</li> <li>gw [&lt;IP&gt; &lt;HOSTNAME&gt;] – Optional. Configures the IPSec secure gateway. When enabling IPSec, you can optionally specify the IPSec secure gateway's numerical IP address or administrator defined hostname.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

```
mint link ip [<IPv4>|<IPv6>|<HOST-ALIAS-NAME>] {<1-65535>|adjacency-hold-time <2-600>|cost <1-10000>|hello-interval <1-120>|level [1|2]|ipsec-security {gw [<IP>|<HOST-NAME>]}}
```

|                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mint</b>                                                    | Configures MiNT protocol parameters required for MiNT link creation and adoption                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>link ip</b><br>[<IPv4>   <IPv6>  <br><HOST-ALIAS-<br>NAME>] | Creates a MiNT routing link <ul style="list-style-type: none"> <li>ip - Creates a MiNT tunnel over UDP/IP or IPv6</li> </ul> <p>Use this keyword to specify the IP address (IPv4 or IPv6) used by peers for inter-operation when supporting the MINT protocol.</p> <ul style="list-style-type: none"> <li>&lt;IPv4&gt; - Specify the IPv4 address used by peers.</li> <li>&lt;IPv6&gt; - Specify the IPv6 address used by peers.</li> <li>&lt;HOST-ALIAS-NAME&gt; - Specify the host alias identifying the MiNT tunnel peer's address. The host alias should existing and configured.</li> </ul> |
| <b>&lt;1-65535&gt;</b>                                         | Select the peer UDP port from 1 - 65535.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>adjacency-hold-time &lt;2-600&gt;</b>                       | Optional. Specifies the adjacency lifetime after hello packets cease <ul style="list-style-type: none"> <li>&lt;2-600&gt; - Specify a value from 2 - 600 seconds. The default is 46 seconds.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>cost &lt;1-100000&gt;</b>                                   | Optional. Specifies the link cost in arbitrary units <ul style="list-style-type: none"> <li>&lt;1-100000&gt; - Specify a value from 1 - 100000. The default is 100.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>hello-interval &lt;1-120&gt;</b>                            | Optional. Specifies the interval, in seconds, between successive hello packets <ul style="list-style-type: none"> <li>&lt;1-120&gt; - Specify a value from 1 - 120. The default is 15 seconds.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>level [1 2]</b>                                             | Optional. Specifies the routing levels for this routing link. The options are: <ul style="list-style-type: none"> <li>1 - Configures local routing</li> <li>2 - Configures inter-site routing</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>ipsec-security</b><br>{gw [<IP>  <br><HOST-NAME>]}          | Optional. Enables IPsec secure peer authentication on the MiNT connection (link). This option is disabled by default. <ul style="list-style-type: none"> <li>gw [&lt;IP&gt; &lt;HOSTNAME&gt;] - Optional. Configures the IPsec secure gateway. When enabling IPsec, you can optionally specify the IPsec secure gateway's numerical IP address or administrator defined hostname.</li> </ul>                                                                                                                                                                                                     |

```
mint mlcp [ip|ipv6|vlan]
```

|                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mint</b>                      | Configures MiNT protocol parameters required for MiNT link creation and adoption                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>mlcp [ip ipv6  <br/>vlan]</b> | Configures the MLCP using the IP address or VLAN. MLCP is used to create a UDP/IP link from the device to a neighbor. The neighboring device does not need to be a wireless controller or service platform, it can be another access point with a path to the wireless controller or service platform. <ul style="list-style-type: none"> <li>vlan - Enables MLCP over layer 2 (VLAN) links</li> <li>ip - Enables MLCP over layer 3 (UDP/IP) links. When enabled, allows adoption over IPv4 address.</li> <li>ipv6 - Enables MLCP over layer 3 (UDP/IPv6) links. When enabled, allows adoption over IPv6 address.</li> </ul> |

```
mint rate-limit level2 [link [ip [<IPv4>|<IPv6>] <1-65535>|vlan <1-4094>] mlcp [ip|ipv6 |
vlan]] rate <50-1000000> max-burst-size <2-1024> {red-threshold [background|best-effort |
video|voice] <0-100>}
```

|                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mint</b>                                                              | Configures MiNT protocol parameters required for MiNT link creation and adoption                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>mint rate-limit level2</b>                                            | <p>Applies rate limits on extended VLAN traffic</p> <p>Excessive traffic can cause performance issues on an extended VLAN. Excessive traffic can be caused by numerous sources including network loops, faulty devices, or malicious software.</p> <p>Rate limiting reduces the maximum rate sent or received per wireless client. It prevents any single user from overwhelming the wireless network, and also provides differential service for service providers. Uplink and downlink rate limits are usually configured on a RADIUS server using vendor specific attributes. Rate limits are extracted from the RADIUS server's response. When such attributes are not present, the settings defined on the controller, service platform or access point are applied. You can set separate QoS rate limit configurations for data types transmitted from the network (upstream) and data transmitted from a wireless clients back to associated radios (downstream).</p> |
| <b>link [ip &lt;IPv4/IPv6&gt; &lt;1-65535&gt;   vlan &lt;1-4094&gt;]</b> | <p>Configures rate limit parameters applicable for all statically configured MiNT links on level2. Select the link-type as 'IP' or 'VLAN'.</p> <ul style="list-style-type: none"> <li>ip &lt;IPv4/IPv6&gt; - Configures rate limits for MiNT link traffic over UDP/IP <ul style="list-style-type: none"> <li>&lt;IPv4/IPv6&gt; - Specify the MiNT peer's IPv4 or IPV6 address in the A.B.C.D and X:X::X:X formats respectively.</li> <li>&lt;1-65535&gt; - Configures the virtual port used for rate limiting traffic. Specify the UDP port from 1 - 65535.</li> </ul> </li> <li>vlan &lt;1-4094&gt; - Configures rate limits for MiNT link traffic on specified VLAN <ul style="list-style-type: none"> <li>&lt;1-4094&gt; - Specify the VLAN ID from 1 - 4094.</li> </ul> </li> </ul>                                                                                                                                                                                      |
| <b>mlcp [ip ipv6   vlan]</b>                                             | <p>Configures rate limit parameters applicable for MLCP</p> <p>MLCP creates a UDP/IP link from the device to a neighbor. The neighboring device does not need to be a controller or service platform, it can be an access point with a path to the controller or service platform.</p> <ul style="list-style-type: none"> <li>ip - Configures rate-limits for MLCP over UDP/IPv4 links</li> <li>ipv6 - Configures rate-limits for MLCP over UDP/IPv6 links</li> <li>vlan - Configures rate-limits for MLCP over VLAN links</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>rate &lt;50-1000000&gt;</b>                                           | <p>Configures the rate limit from 50 - 1000000 Kbps</p> <p>This limit constitutes a threshold for the maximum number of packets transmitted or received (from all access categories). Traffic exceeding the defined rate is dropped and a log message is generated. The default setting is 5000 Kbps.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

|                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>max-burst-size</b><br><b>&lt;2-1024&gt;</b>                                                                        | Configures the maximum burst size from 0 - 1024 Kbytes<br>Smaller the burst size, lesser is the probability of the upstream packet transmission resulting in congestion for the WLAN's client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, add a 10% margin (minimally) to allow for traffic bursts. The default burst size is 320 Kbytes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>red-threshold</b><br><b>[background  </b><br><b>best-effort  </b><br><b>video   voice]</b><br><b>&lt;0-100&gt;</b> | Optional. Configures the random early detection (RED) threshold (as a percentage) for the following traffic types: <ul style="list-style-type: none"> <li>• background – Configures the RED threshold for low priority background traffic. Background packets are dropped and a log message generated if the rate exceeds the set value. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis). The default setting is 50%.</li> <li>• best-effort – Configures the RED threshold for low priority best-effort traffic. Best-effort packets are dropped and a log message generated if the rate exceeds the set value. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis).The default setting is 50%.</li> <li>• video – Configures the RED threshold for high priority video traffic. Video packets are dropped and a log message generated if the rate exceeds the set value. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis).The default setting is 25%.</li> <li>• voice – Configures the RED threshold for high priority voice traffic. Voice packets are dropped and a log message generated if the rate exceeds the set value. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis).The default setting is 0%. <ul style="list-style-type: none"> <li>• &lt;0-100&gt; – After selecting the traffic type, specify the RED threshold from 0 - 100%.</li> </ul> </li> </ul> |

```
mint spf-latency <0-60>
```

|                                           |                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mint</b>                               | Configures MiNT protocol parameters required for MiNT link creation and adoption                                                                                                                                                                                                                                              |
| <b>spf-latency</b><br><b>&lt;0-60&gt;</b> | Specifies the latency of SPF routing recalculation<br>This option allows you to set the latency of routing recalculation option (within the Shortest Path First (SPF) field). This option is disabled by default. <ul style="list-style-type: none"> <li>• &lt;0-60&gt; – Specify the latency from 0 - 60 seconds.</li> </ul> |

```
mint tunnel-across-extended-vlan
```

|                                    |                                                                                                          |
|------------------------------------|----------------------------------------------------------------------------------------------------------|
| <b>mint</b>                        | Configures MiNT protocol parameters required for MiNT link creation and adoption                         |
| <b>tunnel-across-extended-vlan</b> | Enables tunneling of MiNT protocol packets across an extended VLAN. This setting is disabled by default. |

```
mint tunnel-controller-load-balancing level1
```



|                         |                                                                                                                                                          |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mint</b>             | Configures MiNT protocol parameters required for MiNT link creation and adoption                                                                         |
| <b>tunnel-</b>          | Enables load balancing of MiNT extended VLAN traffic across tunnels                                                                                      |
| <b>controller-load-</b> | <ul style="list-style-type: none"> <li>level1 - Enables balancing of load of a tunnel wireless controller or service platform over VLAN links</li> </ul> |
| <b>balancing level1</b> |                                                                                                                                                          |

### Example

```

nx9500-6C8809(config-profile-default-rfs4000)#mint level 1 area-id 88

nx9500-6C8809(config-profile-default-rfs4000)#mint link ip 1.2.3.4 level 2

nx9500-6C8809(config-profile-default-rfs4000)#show context
profile rfs4000 default-rfs4000
 mint link ip 1.2.3.4 level 2
 mint level 1 area-id 88
 bridge vlan 1
--More--
nx9500-6C8809(config-profile-default-rfs4000)#

nx9500-6C8809(config-device-84-24-8D-1B-B9-0C)#show context
ap7522 84-24-8D-1B-B9-0C
 use profile default-ap7522
 use rf-domain default
 hostname ap7522-1BB90C
 no staging-config-learnt
nx9500-6C8809(config-device-84-24-8D-1B-B9-0C)

nx9500-6C8809(config-device-84-24-8D-1B-B9-0C)#mint inter-tunnel-bridging

nx9500-6C8809(config-device-84-24-8D-1B-B9-0C)#show context
ap7522 84-24-8D-1B-B9-0C
 use profile default-ap7522
 use rf-domain default
 hostname ap7522-1BB90C
 no staging-config-learnt
 mint inter-tunnel-bridging
nx9500-6C8809(config-device-84-24-8D-1B-B9-0C)#

```

### Related Commands

|                        |                                               |
|------------------------|-----------------------------------------------|
| <b>no</b> on page 1200 | Disables or reverts settings to their default |
|------------------------|-----------------------------------------------|

*misconfiguration-recovery-time*

[Profile Config Commands](#) on page 862

Verifies connectivity after a configuration is received

#### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

## Syntax

```
misconfiguration-recovery-time [0|<60-300>]
```

## Parameters

```
misconfiguration-recovery-time [0|<60-300>]
```

|                       |                                                                       |
|-----------------------|-----------------------------------------------------------------------|
| <b>&lt;60-300&gt;</b> | Sets the recovery time from 60 - 300 seconds (default is 180 seconds) |
| <b>0</b>              | Disables recovery from misconfiguration                               |

## Example

```
NOC-NX9500(config-profile-testNX9000)#misconfiguration-recovery-time 65
```

```
NOC-NX9500(config-profile-testNX9000)#show context include-factory | include mis
configuration-recovery-time
 misconfiguration-recovery-time 65
 min-misconfiguration-recovery-time 500
NOC-NX9500(config-profile-testNX9000)#
```

## Related Commands

|                        |                                  |
|------------------------|----------------------------------|
| <b>no</b> on page 1200 | Reverts to default (180 seconds) |
|------------------------|----------------------------------|

## *neighbor-inactivity-timeout*

[Profile Config Commands](#) on page 862

Configures neighbor inactivity timeout

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

## Syntax

```
neighbor-inactivity-timeout <1-1000>
```

## Parameters

```
neighbor-inactivity-timeout <1-1000>
```

|                       |                                                                                                                                                                       |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;1-1000&gt;</b> | Sets neighbor inactivity timeout <ul style="list-style-type: none"><li>• &lt;1-1000&gt; - Specify a value from 1 - 1000 seconds. The default is 30 seconds.</li></ul> |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Example

```
nx9500-6C8809(config-profile-default)#neighbor-inactivity-timeout 500
```

```
nx9500-6C8809(config-profile-default-rfs4000)#show context
profile rfs4000 default-rfs4000
 mint link ip 1.2.3.4
 mint level 1 area-id 88
```

```

bridge vlan 1
 bridging-mode isolated-tunnel
 ip igmp snooping
 ip igmp snooping querier
neighbor-inactivity-timeout 500
autoinstall configuration
autoinstall firmware
crypto ikev1 policy ikev1-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ikev2 policy ikev2-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
crypto ikev1 remote-vpn
crypto ikev2 remote-vpn
crypto auto-ipsec-secure
interface mel
interface gel
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
--More--
nx9500-6C8809(config-profile-default-rfs4000)#

```

### *neighbor-info-interval*

[Profile Config Commands](#) on page 862

Configures the neighbor information exchange interval

#### **Supported in the following platforms:**

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### **Syntax**

```
neighbor-info-interval <1-100>
```

#### **Parameters**

```
neighbor-info-interval <1-100>
```

|                      |                                                                |
|----------------------|----------------------------------------------------------------|
| <b>&lt;1-100&gt;</b> | Sets interval from 1 - 100 seconds. The default is 10 seconds. |
|----------------------|----------------------------------------------------------------|

#### **Example**

```
nx9500-6C8809(config-profile-default-rfs4000)#neighbor-info-interval 6
```

```

nx9500-6C8809(config-profile-default-rfs4000)#show context
profile rfs4000 default-rfs4000
 mint link ip 1.2.3.4
 mint level 1 area-id 88
 bridge vlan 1
 bridging-mode isolated-tunnel
 ip igmp snooping
 ip igmp snooping querier
 neighbor-info-interval 6
 neighbor-inactivity-timeout 500

```

```

autoinstall configuration
autoinstall firmware
crypto ikev1 policy ikev1-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ikev2 policy ikev2-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
crypto ikev1 remote-vpn
crypto ikev2 remote-vpn
crypto auto-ipsec-secure
interface me1
interface ge1
 ip dhcp trust
 qos trust dscp
--More--
nx9500-6C8809(config-profile-default-rfs4000)#

```

no

[Profile Config Commands](#) on page 862

Negates a command or resets values to their default

#### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```

no [adopter-auto-provisioning-policy-lookup|adoption|adoption-mode|alias|
application-policy|area|arp|auto-learn|autogen-uniqueid|autoinstall|
bluetooth-detection|bridge|cdp|cluster|configuration-persistence|
controller|critical-resource|crypto|database-backup|device-upgrade|diag|
dot1x|dpi|dscp-mapping| eguest-server|email-notification|environmental-
sensor|events|export|file-sync|floor|gre|http-analyze|interface|ip|ipv6|
lACP|l2tpv3|l3e-lite-table|led| led-timeout|legacy-auto-downgrade|legacy-
auto-update|lldp|load-balancing| logging|mac-address-table|mac-auth|
management-server|memory-profile| meshpoint-device|meshpoint-monitor-
interval|min-misconfiguration-recovery-time| mint|misconfiguration-
recovery-time|noc|ntp|otls|offline-duration|power-config|preferred-
controller-group|preferred-tunnel-controller|radius|raid| rf-domain-
manager|router|spanning-tree|traffic-class-mapping|traffic-shape|
trustpoint|tunnel-controller|use|virtual-controller|vrrp|vrrp-state-
check|zone| wep-shared-key-auth|service]

```

#### Parameters

no <PARAMETERS>

|                           |                                                                           |
|---------------------------|---------------------------------------------------------------------------|
| <b>no</b>                 | Removes or reverts this profile's settings based on the parameters passed |
| <b>&lt;PARAMETERS&gt;</b> |                                                                           |

## Usage Guidelines

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

### Example

```
nx9500-6C8809(config-profile-default-rfs4000)#show context
profile rfs4000profile rfs4000 default-rfs4000
 autoinstall configuration
 autoinstall firmware
 crypto ikev1 policy ikev1-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 crypto remote-vpn-client
 interface me1
 interface up1
 interface ge1
 interface ge2
 interface ge3
 interface ge4
 interface ge5
 interface ge6
 interface ge7
 interface ge8
 interface wwan1
 interface pppoe1
 use firewall-policy default
 logging on
 service pm sys-restart
 adopter-auto-provisioning-policy-lookup
 router ospf
 router bgp
 adoption start-delay min 10 max 30
nx9500-6C8809(config-profile-default-rfs4000)#

nx9500-6C8809(config-profile-default-rfs4000)#no adopter-auto-provisioning-policy-lookup
nx9500-6C8809(config-profile-default-rfs4000)#no adoption start-delay

nx9500-6C8809(config-profile-default-rfs4000)#show context
profile rfs4000 default-rfs4000
 autoinstall configuration
 autoinstall firmware
 crypto ikev1 policy ikev1-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 crypto remote-vpn-client
 interface me1
 interface up1
 interface ge1
 interface ge2
 interface ge3
 interface ge4
 interface ge5
```

```

interface ge6
interface ge7
interface ge8
interface wwan1
interface pppoe1
use firewall-policy default
logging on
service pm sys-restart
router ospf
router bgp
nx9500-6C8809(config-profile-default-rfs4000)#

```

*noc*

[Profile Config Commands](#) on page 862

Configures Network Operations Center (NOC) statistics update interval. This is the interval at which statistical updates are sent by the RF Domain manager to its adopting controller (the NOC controller).

**Supported in the following platforms:**

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
noc update-interval [<5-3600>|auto]
```

**Parameters**

```
noc update-interval [<5-3600>|auto]
```

|                                                   |                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>noc update-interval</b><br>[<5-3600> <br>auto] | <p>Configures NOC statistics update interval</p> <ul style="list-style-type: none"> <li>• &lt;5-3600&gt; - Specify the update interval from 5 - 3600 seconds.</li> <li>• auto - The NOC statistics update interval is automatically adjusted by the wireless controller or service platform based on load. This option is enabled by default.</li> </ul> |
|---------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Example**

```

NOC-NX9500(config-profile-testNX9000)#noc update-interval 25

NOC-NX9500(config-profile-testNX9000)#show context include-factory | include noc

 noc update-interval 25
NOC-NX9500(config-profile-testNX9000)#

```

**Related Commands**

|                                 |                               |
|---------------------------------|-------------------------------|
| <a href="#">no</a> on page 1200 | Resets NOC related parameters |
|---------------------------------|-------------------------------|

*nsight*

[Profile Config Commands](#) on page 862

Configures NSight database related parameters. Use this command to configure the data-update periodicity, number of applications posted to the NSight server for a wireless client, and the duration for which data is stored in the NSight database's buckets. These parameters impact the amount of data stored in the NSight DB and interval at which data is aggregated and expired within the NSight DB. For more information on data aggregation and expiration, see [Usage Guidelines\(Data Aggregation and Expiration\)](#) on page 1205.

Configure these parameters in the NSight server's profile configuration mode. These parameters are also configurable on the NSight server's device configuration mode.

#### Supported in the following platforms:

- Service Platforms — NX9500, NX9510, NX9600, VX9000

#### Syntax

```
nsight database [statistics|summary]
```

```
nsight database statistics [avc-update-interval|max-apps-per-client|max-http-usage-metadata|max-http-visits-metadata|max-ssl-usage-metadata|max-ssl-visits-metadata|update-interval|wireless-clients-update-interval]
```

```
nsight database statistics [avc-update-interval|update-interval|wireless-clients-update-interval] [120|30|300|60|600]
```

```
nsight database statistics max-apps-per-client <1-1000>
```

```
nsight database statistics [max-http-usage-metadata|max-http-visits-metadata|max-ssl-usage-metadata|max-ssl-visits-metadata] <1-1000>
```

```
nsight database summary duration <1-24> <1-168> <1-2160> <24-26280>
```

#### Parameters

```
nsight database statistics [avc-update-interval|update-interval|wireless-clients-update-interval] [120|30|300|60|600]
```

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>nsight database statistics</b> | Configures NSight database statistics related parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>avc-update-interval</b>        | Configures the interval, in seconds, at which Application Visibility and Control (AVC) statistics is updated to the NSight database. This interval represents the rate at which AVC-related data is inserted in the NSight database's first bucket. This first bucket data is referred to as the RAW records. A bucket is a database collection that holds statistical data on a per RF Domain basis. For more information, see <a href="#">Usage Guidelines (Data Aggregation and Expiration)</a> on page 1274.<br>When configured, RF Domain managers posting AVC-related data to the NSight server receive a reply from the NSight server intimating the next update time. The NSight server calculates the 'next update time' based on the avc-update-interval configured here. |

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>update-interval</b>                  | Configures the interval, in seconds, at which data is updated to the NSight server. This interval represents the rate at which data (excluding AVC and wireless-clients related statistics) is inserted in the NSight database's first bucket. This first bucket data is referred to as the RAW records. A bucket is a database collection that holds statistical data on a per RF Domain basis. For more information, see <a href="#">Usage Guidelines (Data Aggregation and Expiration)</a> on page 1274.                                                                                                                                                                                                                                                                                          |
| <b>contd..</b>                          | When configured, RF Domain managers posting data to the NSight server receive a reply from the NSight server intimating the next update time. The NSight server calculates the 'next update time' based on the update-interval configured here.<br><br><b>Note:</b> Use the 'avc-update-interval' and 'wireless-clients-update-interval' keywords to configure update interval for AVC-related and wireless-clients related information respectively.                                                                                                                                                                                                                                                                                                                                                |
| <b>wireless-clients-update-interval</b> | Configures the interval, in seconds, at which wireless-client statistics is updated to the NSight server. This interval represents the rate at which wireless-clients related statistics is inserted in the NSight database's first bucket. This first bucket data is referred to as the RAW records. A bucket is a database collection that holds statistical data on a per RF Domain basis. For more information, see <a href="#">Usage Guidelines (Data Aggregation and Expiration)</a> on page 1274.<br>When configured, RF Domain managers posting wireless-client related data to the NSight server receive a reply from the NSight server intimating the next update time. The NSight server calculates the 'next update time' based on the wireless-clients-update-interval configured here. |
| <b>[120   30   300   60   600]</b>      | The following keywords are common to all of the above parameters: <ul style="list-style-type: none"> <li>• 120 – Sets the data-update periodicity as 120 seconds (2 minutes)</li> <li>• 30 – Sets the data-update periodicity as 30 seconds</li> <li>• 300 – Sets the data-update periodicity as 300 seconds (5 minutes). This is the default setting for the 'avc-update-interval' and 'wireless-clients-update-interval' parameters.</li> <li>• 60 – Sets the data-update periodicity as 60 seconds (1 minute). This is the default setting for the 'update-interval' parameter.</li> <li>• 600 – Sets the data-update periodicity as 600 seconds (10 minutes)</li> </ul>                                                                                                                          |

```
nsight database statistics max-apps-per-client <1-1000>
```

|                                   |                                                                                                                                                                                                                                                       |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>nsight database statistics</b> | Configures NSight database statistics related parameters                                                                                                                                                                                              |
| <b>max-apps-per-client</b>        | Configures the maximum number of applications per wireless-client to be posted to the NSight server within the configured data-update interval. This information is included in the AVC statistics posted by RF Domain managers to the NSight server. |
| <b>&lt;1-1000&gt;</b>             | Specify the number of applications posted from 1 - 1000. The default is 10 applications per wireless client.                                                                                                                                          |

```
nsight database statistics [max-http-usage-metadata|max-http-visits-metadata | max-ssl-usage-metadata|max-ssl-visits-metadata] <1-1000>
```



|                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>nsight database statistics</b>                                                                              | Configures NSight database statistics related parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>[max-http-usage-metadata   max-http-visits-metadata   max-ssl-usage-metadata   max-ssl-visits-metadata]</b> | <p>Configures the number of HTTP and/or SSL metadata posted within an update interval</p> <ul style="list-style-type: none"> <li>max-http-usage-metadata – Configures the NSight database maximum http-metadata by usage (rx+tx) to be posted in an update-interval</li> <li>max-http-visits-metadata – Configures the NSight database’s maximum http-metadata by the number of visits to be posted within an update-interval</li> <li>max-ssl-usage-metadata – Configures the NSight database maximum ssl-metadata by usage (rx+tx) to be posted in an update-interval</li> </ul> |
| <b>contd...</b>                                                                                                | <ul style="list-style-type: none"> <li>max-ssl-visits-metadata – Configures the NSight database’s maximum ssl-metadata by the number of visits to be posted within an update-interval</li> </ul> <p>The following keyword is common to all of the above mentioned metadata options:</p> <ul style="list-style-type: none"> <li>&lt;1-1000&gt; – Specify a value from 1 - 1000. The default is 10 metadata for each.</li> </ul>                                                                                                                                                     |

nsight database summary duration <1-24> <1-168> <1-2160> <24-26280>

|                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>nsight database summary</b>                                             | Configures the NSight database’s per-bucket data storage duration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>duration &lt;1-24&gt; &lt;1-168&gt; &lt;1-2160&gt; &lt;24-26280&gt;</b> | <p>Configures the duration for which data is stored on a per-bucket basis</p> <ul style="list-style-type: none"> <li>&lt;1-24&gt; – Specify the bucket 1 duration from 1 - 24 hours (i.e. 1 hour to 1 day). The default is 8 hours.</li> <li>&lt;1-168&gt; – Specify the bucket 2 duration from 1 - 168 hours (i.e. 1 hour to 7 days). The default is 24 hours.</li> <li>&lt;1-2160&gt; – Specify the bucket 3 duration from 1 - 2160 hours (i.e. 1 hour to 90 days). The default is 7 days (168 hours).</li> <li>&lt;24-26280&gt; – Specify the bucket 4 duration from 24 - 26280 hours (i.e. 1 day to 3 years). The default is 365 days (1 year).</li> </ul> <p>A bucket is a database collection that holds statistical data for each RF Domain within the network. (Note, only those RF Domain’s that are using an NSight policy with the NSight server host configured will post data to the NSight server. (For more information, see <a href="#">use (rf-domain-config-mode)</a> on page 524 in the RF Domain configuration mode.) NSight database has four (4) buckets. The data from each bucket is aggregated and pushed to the next bucket once the data storage duration, specified for the bucket, has exceeded. For more information on data aggregation, see <a href="#">Usage Guidelines (Data Aggregation and Expiration)</a> on page 1274.</p> |

### Usage Guidelines(Data Aggregation and Expiration)

Data Aggregation:

The NSight functionality, a data analytics tool, analyzes data that is generated periodically by the nodes within the managed wireless LAN. For large WLAN networks, generating significantly large amount of data, storing data forever is neither feasible nor beneficial. Therefore, older statistics are summarized into aggregated (averaged) records. All records, for a fixed time period in past, are summarized into one record by taking an average of them. Although this causes a loss in the data’s granularity, average numbers for any given time period is still available.

---

Statistical data periodically posted by RF Domain managers to the NSight server are stored in buckets (database collections) within the NSight database. There are four buckets in total. These are:

- First bucket (termed as the RAW bucket) - B1
- Second bucket - B2
- Third bucket - B3
- Fourth bucket - B4

On completion of the data storage duration, records from a bucket are aggregated (at a fixed rate) and inserted into the next bucket. The rate at which records are aggregated into the next bucket becomes the next bucket's granularity. For example, the B1 records (that have exceeded the data storage duration configured for B1) are aggregated (at the rate specified) and inserted into B2. Similarly, data from B2 are aggregated into B3, and from B3 to B4. The fixed rate of aggregation (or granularity) AND default storage duration for each bucket is as follows:

- B1: storage duration 8 hours
- B2: granularity 10 minutes / storage duration 24 hours
- B3: granularity 1 hour / storage duration 7 days
- B4: granularity 1 day / storage duration 1 year

Let us consider (with default update-interval settings) the growth of any one of the statistical buckets.

- Since B1's default data storage duration is 8 hours, B1 will hold a maximum of 960 records per RF Domain after 8 hours (updated at the rate of 30 seconds).
- Since B2's granularity is 10 minutes, every 10 minutes 20 records from the B1 will be aggregated into a single record and inserted into B2.
- Since B2's default storage duration is 24 hours, it will contain a maximum of 144 records per RF Domain after 24 hours.
- Since B3's granularity is 1 hour, every hour 6 records from B2 will be aggregated into a single record and inserted into B3.
- Since B3's default storage duration is 7 days, it will contain a maximum of 168 records per RF Domain after 7 days.
- Since B4's granularity is 1 day, every day 24 records from B3 will be aggregated into a single record and inserted into B4.
- Since B4's default storage duration is 365 days, it will contain a maximum of 365 records per RF Domain after 1 year.

Data Expiration:

The expiration of older records (also referred to as purging or deleting of records) occurs along with data aggregation for each bucket.

Let us consider (with default data storage-duration settings) the expiration of data for any one of the statistical buckets.

- As stated earlier, at the end of 8 hours B1 will have 960 records per RF Domain. After a period of 8 hours and 10 minutes, all 960 records are aggregated into 144 records and inserted into B2. To enable B1 to hold exactly 8 hours worth of data, 20 of the oldest records (corresponding to the first

10 minutes) are purged from B1 at the end of 8 hours and 10 minutes. This expiration cycle is triggered every 10 minutes.

- At the end of 24 hours B2 will have 144 records per RF Domain. After a period of 24 hours and 10 minutes, one of the oldest record (corresponding to the first 10 minutes) is purged from B2. This expiration cycle is triggered every 10 minutes to enable B2 to maintain exactly 24 hours worth of data.
- At the end of 7 days B3 will have 168 records per RF Domain. After a period of 7 days and one hour one of the oldest record (corresponding to the first hour) is purged from B3. This expiration cycle is triggered every 1 hour to enable B3 to maintain exactly 7 days worth of data.
- At the end of 365 days B4 will have 365 records per RF Domain. After 365 days, the oldest records (corresponding to the first day) are purged from B4. This expiration cycle is triggered every 1 day to enable B4 to maintain exactly 365 days worth of data.

### Example

```
nx9500-6C8809(config-profile-testNX9500)#nsight database statistics avc-update-interval
120

nx9500-6C8809(config-profile-testNX9500)#nsight database statistics update-interval 30

nx9500-6C8809(config-profile-testNX9500)#nsight database statistics wireless-clients-
update-interval 600

nx9500-6C8809(config-profile-testNX9500)#nsight database statistics max-apps-per-client 20

nx9500-6C8809(config-profile-testNX9500)#nsight database summary duration 12 30 200 500

nx9500-6C8809(config-profile-testNX9500)#show context include-factory | include nsight
use nsight-policy nsight-noc
nsight database statistics update-interval 30
nsight database statistics wireless-clients-update-interval 600
nsight database summary duration 12 30 200 500
nsight database statistics avc-update-interval 120
nsight database statistics max-apps-per-mu 20
nx9500-6C8809(config-profile-testNX9500)#
```

### Related Commands

|                                 |                                                                             |
|---------------------------------|-----------------------------------------------------------------------------|
| <a href="#">no</a> on page 1271 | Reverts the NSight database related parameters configured to default values |
|---------------------------------|-----------------------------------------------------------------------------|

*ntp*

[Profile Config Commands](#) on page 862

Configures the Network Time Protocol (NTP) server settings

NTP manages time and/or network clock synchronization within the network. NTP is a client/server implementation. Controllers, service platforms, and access points (NTP clients) periodically synchronize their clock with a master clock (an NTP server). For example, a controller resets its clock to 07:04:59 upon reading a time of 07:04:59 from its designated NTP server.

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000

- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
ntp server <PEER-IP/HOSTNAME> {autokey|key|maxpoll|minpoll|prefer|version}
```

```
ntp server <PEER-IP/HOSTNAME> {autokey}
```

```
ntp server <PEER-IP/HOSTNAME> {maxpoll [1024|2048|4096|8192]}
```

```
ntp server <PEER-IP/HOSTNAME> {minpoll [1024|128|256|512|64]}
```

```
ntp server <PEER-IP> {key <1-65534> md5 [0 <WORD>|2<WORD>|<WORD>]}
```

```
ntp server <PEER-IP/HOSTNAME> {prefer version <1-4>|version <1-4> prefer}
```

### Parameters

```
ntp server <PEER-IP/HOSTNAME> {autokey} {prefer version <1-4>|version <1-4>}
```

|                                            |                                                                                                                                                                                                                                                                       |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ntp server &lt;PEER-IP/HOSTNAME&gt;</b> | Configures NTP server resources that are used to obtain system time <ul style="list-style-type: none"> <li>• &lt;PEER-IP/HOSTNAME&gt; - Identifies the NTP server resource by its IP address or hostname. Specify the NTP server's IP address or hostname.</li> </ul> |
| <b>autokey</b>                             | Optional. Enables automatic configuration of authentication key for the specified NTP server. This option is disabled by default. If not enabled, use the 'key' option to configure an authentication key for the NTP server.                                         |

```
ntp server <PEER-IP/HOSTNAME> {maxpoll [1024|2048|4096|8192]}
```

|                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ntp server &lt;PEER-IP/HOSTNAME&gt;</b> | Configures NTP server resources that are used to obtain system time <ul style="list-style-type: none"> <li>• &lt;PEER-IP/HOSTNAME&gt; - Identifies the NTP server resource by its IP address or hostname. Specify the NTP server's IP address or hostname.</li> </ul>                                                                                                                                                                                                                                                                                   |
| <b>maxpoll [1024 2048 4096 8192]</b>       | Optional. Configures the maximum polling interval. Once set, the specified NTP server is polled no later than the defined interval. Select one of the following options: <ul style="list-style-type: none"> <li>• 1024 - Configures the maximum polling interval as 1024 seconds. This is the default setting.</li> <li>• 2048 - Configures the maximum polling interval as 2048 seconds</li> <li>• 4096 - Configures the maximum polling interval as 4096 seconds</li> <li>• 8192 - Configures the maximum polling interval as 8192 seconds</li> </ul> |

```
ntp server <PEER-IP/HOSTNAME> {minpoll [1024|128|256|512|64]}
```

|                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ntp server</b><br><b>&lt;PEER-IP/<br/>HOSTNAME&gt;</b> | Configures NTP server resources that are used to obtain system time <ul style="list-style-type: none"> <li>• &lt;PEER-IP/HOSTNAME&gt; - Identifies the NTP server resource by its IP address or hostname. Specify the NTP server's IP address or hostname.</li> </ul>                                                                                                                                                                                                                                                                                                                                                    |
| <b>minpoll [1024  <br/>128   256   512  <br/>64]</b>      | Optional. Configures the minimum polling interval. Once set, the specified NTP server is polled no sooner than the defined interval. Select one of the following options: <ul style="list-style-type: none"> <li>• 1024 - Configures the minimum polling interval as 1024 seconds</li> <li>• 128 - Configures the minimum polling interval as 128 seconds</li> <li>• 256 - Configures the minimum polling interval as 256 seconds</li> <li>• 512 - Configures the minimum polling interval as 512 seconds</li> <li>• 64 - Configures the minimum polling interval as 64 seconds. This is the default setting.</li> </ul> |

```
ntp server <PEER-IP/HOSTNAME> {key <1-65534> md5 [0 <WORD> | 2<WORD> | <WORD>]}
```

|                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ntp server</b><br><b>&lt;PEER-IP/<br/>HOSTNAME&gt;</b>                                   | Configures NTP server resources that are used to obtain system time <ul style="list-style-type: none"> <li>• &lt;PEER-IP/HOSTNAME&gt;&gt; - Identifies the NTP server resource by its IP address or hostname. Specify the NTP server's IP address or hostname.</li> </ul>                                                                                                                                                                                                                                                                                              |
| <b>key &lt;1-65534&gt;<br/>md5 [0 &lt;WORD&gt;  <br/>2 &lt;WORD&gt;  <br/>&lt;WORD&gt;]</b> | Optional. Defines the authentication key for the specified NTP server. This option is used to configure the key when 'autokey' configuration is not enabled. <ul style="list-style-type: none"> <li>• &lt;1-65534&gt; - Specify the peer key number. Should not exceed 64 characters in length.</li> <li>• md5 - Sets MD5 authentication <ul style="list-style-type: none"> <li>0 &lt;WORD&gt; - Configures a clear text password</li> <li>2 &lt;WORD&gt; - Configures an encrypted password</li> <li>&lt;WORD&gt; - Sets an authentication key</li> </ul> </li> </ul> |

```
ntp server <PEER-IP/HOSTNAME> {prefer version <1-4> | version <1-4> prefer}
```

|                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ntp server</b><br><b>&lt;PEER-IP/<br/>HOSTNAME&gt;</b> | Configures NTP server resources that are used to obtain system time <ul style="list-style-type: none"> <li>• &lt;PEER-IP/HOSTNAME&gt; - Identifies the NTP server resource by its IP address or hostname. Specify the NTP server's IP address or hostname.</li> </ul>                                                                                                                                                                                                                                                                     |
| <b>prefer version<br/>&lt;1-4&gt;</b>                     | Optional. Designates the specified NTP server as a preferred NTP resource. This setting is disabled by default. <ul style="list-style-type: none"> <li>• version - Optional. Configures the NTP version <ul style="list-style-type: none"> <li>• &lt;1-4&gt; - Select the NTP version from 1 - 4. If not specified, the default value of '0' is applied, which implies that the NTP server's version is ignored.</li> </ul> </li> </ul>                                                                                                   |
| <b>version &lt;1-4&gt;<br/>prefer</b>                     | Optional. Configures the version number used by the specified NTP server resource <ul style="list-style-type: none"> <li>• &lt;1-4&gt; - Select the NTP version from 1 - 4. The default setting is 0. A value of '0' implies that the NTP server's version is ignored.</li> <li>• prefer - Optional. Designates the specified NTP server as a preferred NTP resource. This setting is disabled by default. The NTP version number specified using the 'version &lt;1-4&gt;' keyword is applied to this preferred NTP resource.</li> </ul> |

### Example

```
NOC-NX9500(config-profile-testNX9000)#ntp server 10.234.160.5
```

```
NOC-NX9500(config-profile-testNX9000)#show context include-factory | include ntp
```

```
no ntp autokey
```

```
no ntp authenticate
ntp server 10.234.160.5
NOC-NX9500(config-profile-testNX9000)#
```

### Related Commands

|                 |                                               |
|-----------------|-----------------------------------------------|
| no on page 1200 | Disables or reverts settings to their default |
|-----------------|-----------------------------------------------|

*otls*

[Profile Config Commands](#) on page 862

Enables support for OmniTrail Location Server (OTLS) beacon identification

OmniTrail (offered by OmniTrail technologies) is a Wi-Fi based locationing protocol used in positioning and tracking location solutions. Access points supporting OTLS beacon identification lock their radios to scan channels for beacons with OTLS tags. Beacons received by the access point are matched for the OTLS signature, and in case of a match, the beacons are forwarded to the OTLS server as UDP payload.

Use this command to configure OTLS server details on the AP and enable OTLS data forwarding. Alternately, OTLS parameters can be configured in the AP's profile on the controller or service platform, and pushed to adopted access points. When configured, APs establish connection with the OTLS server and forward OTLS locationing feeds to the server.

### Supported in the following platforms:

- Access Points — AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8432, AP8533

### Syntax

```
otls [apid|control-port|data-port|forward|server-ip]
```

```
otls apid <WORD>
```

```
otls control-port <0-65535>
```

```
otls data-port [2.4GHz|5GHz] <0-65535>
```

```
otls forward [2.4GHz|5GHz] [disable|enable]
```

```
otls server-ip <OTLS-SERVER-IP>
```

### Parameters

```
otls apid <WORD>
```

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>otls apid<br/>&lt;WORD&gt;</b> | Configures a unique identification for the OTLS-enabled access point. The access point identifier (APID) enables the OTLS server to identify the AP forwarding the OTLS tag. <ul style="list-style-type: none"><li>• &lt;WORD&gt; - Specify an ID for the AP.</li></ul> To ensure that OTLS-enabled APs have unique OTLS ID, it is recommended that the APID is configured in the device context of each AP. |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
otls control-port <0-65535>
```

|                                          |                                                                                                                                                                                                            |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>otls control-port &lt;0-65535&gt;</b> | Configures the port used by the AP to establish and maintain connection with the OTLS server <ul style="list-style-type: none"><li>• &lt;0-65535&gt; - Specify the control port from 0 - 655635.</li></ul> |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
otls data-port [2.4GHz|5GHz] <0-65535>
```

|                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>otls data-port [2.4GHz 5GHz] &lt;0-65535&gt;</b> | Configures the port used by the AP to forward OTLS beacons to the OTLS server. However, OTLS data forwarding has to be enabled on the APs. Use the <code>otls &gt; forward &gt; [2.4GHz 5GHz] &gt; [disable enable]</code> command to enable data forwarding. <ul style="list-style-type: none"><li>• 2.4GHz - Configures the port used to forward OTLS beacons received on the 2.4 GHz band</li><li>• 5.0GHz - Configures the port used to forward OTLS beacons received on the 5.0 GHz band</li></ul> The following keyword is common to the above parameters: <ul style="list-style-type: none"><li>• &lt;0-65535&gt; - Specify a data-forwarding port from 0 - 65535.</li></ul> |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
otls forward [2.4GHz|5GHz] [disable|enable]
```

|                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>otls forward [2.4GHz 5GHz] [disable enable]</b> | Enables or disables OTLS tag forwarding <ul style="list-style-type: none"><li>• 2.4GHz - Enables or disables forwarding of OTLS beacons received on the 2.4 GHz band</li><li>• 5GHz - Enables or disables forwarding of OTLS beacons received on the 5.0 GHz band</li></ul> The following keywords are common to the above parameters: <ul style="list-style-type: none"><li>• disable - Disables OTLS tag forwarding. By default OTLS beacon forwarding is disabled for both 2.4 GHz and 5.0 GHz bands.</li><li>• enable - Enables OTLS tag forwarding</li></ul> |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
otls server-ip <OTLS-SERVER-IP>
```

|                                              |                                                                                                                                                          |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>otls server-ip &lt;OTLS-SERVER-IP&gt;</b> | Configures the OTLS server's IP address <ul style="list-style-type: none"><li>• &lt;OTLS-SERVER-IP&gt; - Specify the OTLS server's IP address.</li></ul> |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|

## Example

```
ap8533-84A224(config-device-84-24-8D-84-A2-24)#otls apid 112233
ap8533-84A224(config-device-84-24-8D-84-A2-24)#otls forward 2.4GHz enable
ap8533-84A224(config-device-84-24-8D-84-A2-24)#otls forward 5GHz enable
ap8533-84A224(config-device-84-24-8D-84-A2-24)#otls control-port 8890
ap8533-84A224(config-device-84-24-8D-84-A2-24)#otls data-port 2.4GHz 8888
ap8533-84A224(config-device-84-24-8D-84-A2-24)#otls data-port 5GHz 8889
ap8533-84A224(config-device-84-24-8D-84-A2-24)#otls server-ip 192.168.13.10

ap8533-84A224(config-device-84-24-8D-84-A2-24)#show context include-factory | include otls
otls forward 5GHz enable
otls forward 2.4GHz enable
otls server-ip 192.168.13.10
otls control-port 8890
otls data-port 2.4GHz 8888
otls data-port 5GHz 8889
otls apid 112233
ap8533-84A224(config-device-84-24-8D-84-A2-24)
```

The following example displays OTLS parameters configured on an AP8533 profile:

```
nx9500-6C8809(config-profile-testAP8533)#show context include-factory | include otls
otls forward 5GHz enable
otls forward 2.4GHz enable
otls server-ip 192.168.13.10
otls control-port 8890
otls data-port 2.4GHz 8888
otls data-port 5GHz 8889
otls apid 12345
nx9500-6C8809(config-profile-testAP8533)#
```

### Related Commands

|                              |                                                                               |
|------------------------------|-------------------------------------------------------------------------------|
| <code>no</code> on page 1200 | Removes the OTLS-related parameters configured on an AP or on an AP's profile |
|------------------------------|-------------------------------------------------------------------------------|

### *offline-duration*

[Profile Config Commands](#) on page 862

Sets the duration, in minutes, for which a device remains unadopted before it generates offline event

This command is also supported on the device configuration mode.

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
offline-duration <5-43200>
```

### Parameters

```
offline-duration <5-43200>
```

|                                                   |                                                                    |
|---------------------------------------------------|--------------------------------------------------------------------|
| <b>offline-duration</b><br><b>&lt;5-43200&gt;</b> | Specify a value from 5 - 43200 minutes. The default is 10 minutes. |
|---------------------------------------------------|--------------------------------------------------------------------|

### Example

```
rfs4000-229D58(config-profile-test)#offline-duration 200

rfs4000-229D58(config-profile-test)#show context
profile rfs4000 test
no autoinstall configuration
no autoinstall firmware
crypto ikev1 policy ikev1-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
.....
interface wwan1
interface pppoe1
use firewall-policy default
service pm sys-restart
```



```
router ospf
offline-duration 200
rfs4000-229D58(config-profile-test)#
```

### Related Commands

|                              |                                                     |
|------------------------------|-----------------------------------------------------|
| <code>no</code> on page 1200 | Resets the offline-duration to default (10 minutes) |
|------------------------------|-----------------------------------------------------|

### *power-config*

[Profile Config Commands](#) on page 862

Configures the power option mode. Use this command in the profile configuration mode to configure the transmit output power of access point radios. This command is also available in the device-config mode.

Single radio model access points always operate using a full power configuration. The power management configurations described in this section do not apply to single radio models. When an access point is powered on for the first time, the system determines the power budget available to the access point. If 802.3af is selected, the access point assumes 12.95 watts is available. If the mode is changed, the access point requires a reset to implement the change. If 802.3at is selected, the access point assumes 23 - 26 watts is available.

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
power-config [af-option|at-option|mode]
```

```
power-config [af-option|at-option] [range|throughput]
```

```
power-config mode [auto|3af]
```

### Parameters

```
power-config [af-option|at-option] [range|throughput]
```

|                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>power-config</b>                                       | Configures the power option mode                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>af-option</b><br><b>[range  </b><br><b>throughput]</b> | <p>Configures the 802.3.af power mode option. The options are:</p> <ul style="list-style-type: none"> <li>range – Configures the af power range mode. This mode provides higher power but fewer transmission (tx) chains.</li> </ul> <p>Select range when range is preferred over performance for broadcast/multicast (group) traffic. The data rates used for range are the lowest defined basic rates.</p> <ul style="list-style-type: none"> <li>throughput – Configures the af power throughput mode. This mode provides lower power but has more tx chains. This is the default setting.</li> </ul> <p>Select throughput to transmit packets at the radio's highest defined basic rate (based on the radio's current basic rate settings). This option is optimal in environments where transmission range is secondary to broadcast/multicast transmission performance.</p> |
| <b>at-option</b><br><b>[range  </b><br><b>throughput]</b> | <p>Configures the 802.3 at power mode option. The options are:</p> <ul style="list-style-type: none"> <li>range – Configures the at power range mode. This mode provides higher power but fewer tx chains.</li> </ul> <p>Select range when range is preferred over performance for broadcast/multicast (group) traffic. The data rates used for range are the lowest defined basic rates.</p> <ul style="list-style-type: none"> <li>throughput – Configures the at power throughput mode. This mode provides lower power but has more tx chains. This is the default setting.</li> </ul> <p>Select throughput to transmit packets at the radio's highest defined basic rate (based on the radio's current basic rate settings). This option is optimal in environments where transmission range is secondary to broadcast/multicast transmission performance.</p>                |

power-config mode [auto|3af]

|                                    |                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>power-config</b>                | Configures the power option mode                                                                                                                                                                                                                                                                                                                                          |
| <b>mode [auto  </b><br><b>3af]</b> | <p>Configures the AP power mode</p> <ul style="list-style-type: none"> <li>3af – Forces an AP to power up in the 802.3af power mode</li> <li>auto – Sets the detection auto mode (default setting)</li> </ul> <p>The automatic power-config mode enables an access point to automatically determine the best power configuration based on the available power budget.</p> |

### Example

```

nx9500-6C8809(config-profile-testAP7161)#power-config mode 3af

nx9500-6C8809(config-profile-testAP7161)#power-config af-option range

nx9500-6C8809(config-profile-testAP7161)#show context
profile ap71xx testAP7161
 no autoinstall configuration
 no autoinstall firmware
 power-config mode 3af
 power-config af-option range
 crypto ikev1 policy ikev1-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 --More--
nx9500-6C8809(config-profile-testAP7161)#

```

## Related Commands

|                              |                                                           |
|------------------------------|-----------------------------------------------------------|
| <code>no</code> on page 1200 | Reverts the power mode setting on this profile to default |
|------------------------------|-----------------------------------------------------------|

### *preferred-controller-group*

[Profile Config Commands](#) on page 862

Specifies the controller group preferred for adoption

At adoption, an access point solicits and receives multiple adoption responses from controllers and service platforms available on the network. These adoption responses contain loading policy information the access point uses to select the optimum controller or service platform for adoption. After selecting the controller or service platform, the access point associates with it and optionally obtains an image upgrade and configuration. By default, an auto provisioning policy generally distributes AP adoption evenly amongst available controllers and service platforms. Use this command to specify the controller or service platform preferred for adoption. Once configured, the access point adopts to the specified preferred controller or service platform.

#### **Supported in the following platforms:**

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

#### **Syntax**

```
preferred-controller-group <WORD>
```

#### **Parameters**

```
preferred-controller-group <WORD>
```

|                     |                                                                                                                                                                                                       |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;WORD&gt;</b> | Specify the name of the controller (wireless controller or service platform) group preferred for adoption. Devices using this profile are added, on adoption, to the controller group specified here. |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### **Example**

```
NOC-NX9500(config-profile-testNX9000)#preferred-controller-group testGroup
```

```
NOC-NX9500(config-profile-testNX9000)#show context include-factory | include preferred-controller-group
 preferred-controller-group testGroup
NOC-NX9500(config-profile-testNX9000)#
```

## Related Commands

|                              |                                                      |
|------------------------------|------------------------------------------------------|
| <code>no</code> on page 1200 | Removes the preferred controller group configuration |
|------------------------------|------------------------------------------------------|

### *preferred-tunnel-controller*

[Profile Config Commands](#) on page 862

Configures the tunnel controller's name preferred for tunneling extended VLAN traffic. Devices using this profile will prefer to route their extended VLAN traffic through the specified tunnel controller (wireless controller or service platform).

**Supported in the following platforms:**

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
preferred-tunnel-controller <NAME>
```

**Parameters**

```
preferred-tunnel-controller <NAME>
```

|                                                       |                                      |
|-------------------------------------------------------|--------------------------------------|
| <code>preferred-tunnel-controller &lt;NAME&gt;</code> | Configures the preferred tunnel name |
|-------------------------------------------------------|--------------------------------------|

**Example**

```
nx9500-6C8809(config-profile-default-rfs4000)#preferred-tunnel-controller testtunnel
```

**Related Commands**

|                              |                                            |
|------------------------------|--------------------------------------------|
| <code>no</code> on page 1200 | Removes the preferred tunnel configuration |
|------------------------------|--------------------------------------------|

*radius*

[Profile Config Commands](#) on page 862

Configures device level RADIUS authentication parameters

**Supported in the following platforms:**

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
radius [nas-identifier|nas-port-id] <WORD>
```

**Parameters**

```
radius [nas-identifier|nas-port-id] <WORD>
```



|                                              |                                                                                                                                                                                           |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>radius</b>                                | Configures RADIUS authentication parameters                                                                                                                                               |
| <b>nas-identifier</b><br><b>&lt;WORD&gt;</b> | Specifies the RADIUS Network Access Server (NAS) identifier attribute used by this device <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specifies the NAS identifier</li> </ul> |
| <b>nas-port-id</b><br><b>&lt;WORD&gt;</b>    | Specifies the RADIUS NAS port ID attribute used by this device <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specifies the NAS port ID</li> </ul>                               |

### Example

```

nx9500-6C8809(config-profile-default-rfs4000)#radius nas-port-id 1

nx9500-6C8809(config-profile-default-rfs4000)#radius nas-identifier test

nx9500-6C8809(config-profile-default-rfs4000)#show context
profile rfs4000 default-rfs4000
mint link ip 1.2.3.4
mint level 1 area-id 88
bridge vlan 1
 bridging-mode isolated-tunnel
 ip igmp snooping
 ip igmp snooping querier
radius nas-identifier test
radius nas-port-id 1
neighbor-info-interval 6
neighbor-inactivity-timeout 500
--More--
nx9500-6C8809(config-profile-default-rfs4000)#

```

### Related Commands

|                        |                                               |
|------------------------|-----------------------------------------------|
| <b>no</b> on page 1200 | Disables or reverts settings to their default |
|------------------------|-----------------------------------------------|

## *rf-domain-manager*

[Profile Config Commands](#) on page 862

Configures the RF Domain manager election criteria

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
rf-domain-manager [capable|priority <1-255>]
```

### Parameters

```
rf-domain-manager [capable|priority <1-255>]
```

|                               |                                                                                                                                                                                                                                                                                                                    |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>rf-domain-manager</b>      | Configures the RF Domain manager election criteria                                                                                                                                                                                                                                                                 |
| <b>capable</b>                | Enables devices using this profile capable of being elected as the RF Domain manager. The RF Domain manager stores and provisions configuration and firmware images for other members of the RF Domain. It also updates state changes, if any, to RF Domain members. This option is enabled by default.            |
| <b>priority &lt;1-255&gt;</b> | Assigns a priority value for devices using this profile in the RF Domain manager election process. The higher the number set, higher is the device's priority in the RF Domain manager election process. <ul style="list-style-type: none"> <li>• &lt;1-255&gt; – Select a priority value from 1 - 255.</li> </ul> |

### Example

```
NOC-NX9500(config-profile-testNX9000)#rf-domain-manager capable
```

```
NOC-NX9500(config-profile-testNX9000)#rf-domain-manager capable
```

```
NOC-NX9500(config-profile-testNX9000)#show context include-factory | include rf-
domain-manager
 rf-domain-manager capable
 rf-domain-manager priority 1
NOC-NX9500(config-profile-testNX9000)#
```

### Related Commands

|                                 |                                               |
|---------------------------------|-----------------------------------------------|
| <a href="#">no</a> on page 1200 | Disables or reverts settings to their default |
|---------------------------------|-----------------------------------------------|

## router

[Profile Config Commands](#) on page 862

Enables dynamic routing (BGP and/or OSPF) and enters the routing protocol configuration mode

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000



#### Note

BGP is supported only on RFS4000, NX75XX, and NX 95XX model controllers and service platforms.

The NX 95XX service platforms do not support OSPF routing.

The access points only support OSPF routing.

### Syntax

```
router [bgp|ospf]
```

## Parameters

router [bgp|ospf]

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>router</b> | Enables dynamic routing and enters the routing protocol configuration mode                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>bgp</b>    | <p>Enables BGP dynamic routing and configures relevant settings</p> <p>BGP is an inter-ISP routing protocol, which establishes routing between ISPs. ISPs use BGP to exchange routing and reachability information between Autonomous Systems (AS) on the Internet. BGP uses TCP as its transport protocol, eliminating the need to implement explicit update fragmentation, retransmission, acknowledgement, and sequencing. Routing information exchanged through BGP supports destination based forwarding only. It assumes a router forwards packets based on the destination address carried in the IP header of the packet.</p> <p>An AS is a set of routers under the same administration that use Interior Gateway Protocol (IGP) and common metrics to define how to route packets within the AS.</p> <p>For more information on dynamic BGP routing configurations, see <a href="#">BORDER GATEWAY PROTOCOL</a> on page 1852.</p> |
| <b>ospf</b>   | <p>Enables OSPF dynamic routing and configures relevant settings. Changes configuration mode to router mode</p> <p>OSPF is a link-state IGP. OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets.</p> <p>For more information on dynamic OSPF routing configurations, see <a href="#">ROUTER-MODE</a> on page 1722.</p>                                                                                                                                                                                                                                                                                                  |

## Example

```
nx9500-6C8809(config-profile-default-rfs4000)#router ospf
```

```
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#?
```

```
Router OSPF Mode commands:
```

```
area OSPF area
auto-cost OSPF auto-cost
default-information Distribution of default information
ip Internet Protocol (IP)
network OSPF network
no Negate a command or set its defaults
ospf Ospf
passive Make OSPF Interface as passive
redistribute Route types redistributed by OSPF
route-limit Limit for number of routes handled OSPF process
router-id Router ID

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal
```

```
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#
```

## Related Commands

|                              |                        |
|------------------------------|------------------------|
| <code>no</code> on page 1200 | Disables OSPF settings |
|------------------------------|------------------------|

*spanning-tree*

[Profile Config Commands](#) on page 862

Enables spanning tree commands. Use these commands to configure the errdisable, multiple spanning tree and portfast settings.

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
spanning-tree [errdisable|mst|portfast]
```

```
spanning-tree errdisable recovery [cause bpduguard|interval <10-1000000>]
```

```
spanning-tree mst [<0-15>|cisco-interoperability|enable|forward-time|
hello-time|instance|max-age|max-hops|region|revision]
```

```
spanning-tree mst [<0-15> priority <0-61440>|cisco-interoperability
[enable|disable]|enable|forward-time <4-30>|hello-time <1-10>|instance
<1-15>| max-age <6-40>|max-hops <7-127>|region <LINE>|revision <0-255>]
```

```
spanning-tree portfast [bpdufilter|bpduguard] default
```

### Parameters

```
spanning-tree errdisable recovery [cause bpduguard|interval <10-1000000>]
```

|                                              |                                                                                                                                                                                                    |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>spanning-tree</b>                         | Configures spanning-tree related parameters                                                                                                                                                        |
| <b>errdisable</b>                            | Disables or shuts down ports where traffic is looping, or ports with traffic in one direction                                                                                                      |
| <b>recovery</b>                              | Enables the timeout mechanism for a port to be recovered. This option is disabled by default.                                                                                                      |
| <b>cause</b><br><b>bpduguard</b>             | Specifies the reason for errdisable <ul style="list-style-type: none"><li>• bpduguard - Recovers from errdisable due to bpduguard</li></ul>                                                        |
| <b>interval</b><br><b>&lt;10-1000000&gt;</b> | Specifies the interval after which a port is enabled <ul style="list-style-type: none"><li>• &lt;10-1000000&gt; - Specify a value from 10 - 1000000 seconds. The default is 300 seconds.</li></ul> |

```
spanning-tree mst [<0-15> priority <0-61440>|cisco-interoperability [enable|disable]|
enable|forward-time <4-30>|hello-time <1-10>|instance <1-15>| max-age <6-40>|max-hops
<7-127>|region <LINE>|revision <0-255>]
```



|                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>spanning-tree</b>                                 | Configures spanning-tree related parameters                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>mst</b>                                           | Configures Multiple Spanning Tree (MST) commands<br>The MSTP provides an extension to STP to optimize the usefulness of VLANs. MSTP allows for a separate spanning tree for each VLAN group, and blocks all but one of the possible alternate paths within each spanning tree topology.                                                                                                                                                                                             |
| <b>&lt;0-15&gt;<br/>priority<br/>&lt;0-61440&gt;</b> | Specifies the number of instances required to configure MST. Select a value from 0 -15.<br><ul style="list-style-type: none"> <li>• priority – Sets the bridge priority to the specified value. This value is used to determine the root bridge. Use the no parameter with this command to restore the default bridge priority value.</li> <li>• &lt;0-61440&gt; – Sets the bridge priority in increments (Lower priority indicates greater likelihood of becoming root)</li> </ul> |
| <b>cisco interoperability [enable disable]</b>       | Enables CISCO interoperability<br>Enables interoperability with CISCO's version of MSTP, which is incompatible with standard MSTP. This setting is disabled by default.                                                                                                                                                                                                                                                                                                             |
| <b>enable</b>                                        | Enables MST protocol                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>forward-time<br/>&lt;4-30&gt;</b>                 | Specifies the forwarding delay time in seconds<br><ul style="list-style-type: none"> <li>• &lt;4-30&gt; – Specify a value from 4 - 30 seconds. The default is 15 seconds.</li> </ul>                                                                                                                                                                                                                                                                                                |
| <b>hello-time<br/>&lt;1-10&gt;</b>                   | Specifies the hello BPDU interval in seconds<br><ul style="list-style-type: none"> <li>• &lt;1-10&gt; – Specify a value from 1 - 10 seconds. The default is 2 seconds.</li> </ul>                                                                                                                                                                                                                                                                                                   |
| <b>instance<br/>&lt;1-15&gt;</b>                     | Defines the instance ID to which the VLAN is associated<br><ul style="list-style-type: none"> <li>• &lt;1-15&gt; – Specify an instance ID from 1 - 10.</li> </ul>                                                                                                                                                                                                                                                                                                                   |
| <b>max-age &lt;6-40&gt;</b>                          | Defines the maximum time to listen for the root bridge<br><ul style="list-style-type: none"> <li>• &lt;6-40&gt; – Specify a value from 4 - 60 seconds. The default is 20 seconds.</li> </ul>                                                                                                                                                                                                                                                                                        |
| <b>max-hops<br/>&lt;7-127&gt;</b>                    | Defines the maximum hops when BPDU is valid<br><ul style="list-style-type: none"> <li>• &lt;7-127&gt; – Specify a value from 7 - 127. The default is 20.</li> </ul>                                                                                                                                                                                                                                                                                                                 |
| <b>region &lt;LINE&gt;</b>                           | Specifies the MST region<br><ul style="list-style-type: none"> <li>• &lt;LINE&gt; – Specify the region name.</li> </ul>                                                                                                                                                                                                                                                                                                                                                             |
| <b>revision<br/>&lt;0-255&gt;</b>                    | Sets the MST bridge revision number. This enables the retrieval of configuration information.<br><ul style="list-style-type: none"> <li>• &lt;0-255&gt; – Specify a value from 0 - 255. This default is 0.</li> </ul>                                                                                                                                                                                                                                                               |

spanning-tree portfast [bpdufilter|bpduguard] default

|                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>spanning-tree</b>                                                  | Configures spanning-tree related parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>portfast</b><br><b>[bpdupfilter   bpduguard]</b><br><b>default</b> | <p>Enables PortFast on a bridge</p> <ul style="list-style-type: none"> <li>• bpdupfilter default – Sets the BPDU filter for the port. The BPDU filter is disabled by default.</li> </ul> <p>The spanning tree protocol sends BPDUs from all ports. Enabling the BPDU filter ensures that PortFast enabled ports do not transmit or receive BPDUs.</p> <ul style="list-style-type: none"> <li>• bpduguard default – Guards PortFast ports against BPDU receive. The BPDU guard is disabled by default.</li> </ul> <p>Enabling the BPDU guard means this port will shutdown on receiving a BPDU.</p> <ul style="list-style-type: none"> <li>• default – Enables the BPDU filter and/or BPDU guard on PortFast enabled ports by default</li> </ul> |

### Usage Guidelines

If a bridge does not hear BPDUs from the root bridge within the specified interval, assume the network has changed and recomputed the spanning-tree topology.

Generally, spanning tree configuration settings in the config mode define the configuration for bridge and bridge instances.

MSTP is based on instances. An instance is a group of VLANs with a common spanning tree. A single VLAN cannot be associated with multiple instances.

Wireless Controllers or service platforms with the same instance, VLAN mapping, revision number and region names define a unique region. Wireless Controllers or service platforms in the same region exchange BPDUs with instance record information within.

### Example

```

nx9500-6C8809(config-profile-default-rfs4000)#spanning-tree errdisable recovery cause
bpduguard

nx9500-6C8809(config-profile-default-rfs4000)#spanning-tree mst 2 priority 4096

nx9500-6C8809(config-profile-default-rfs4000)#show context
profile rfs4000 default-rfs4000
mint link ip 1.2.3.4
mint level 1 area-id 88
bridge vlan 1
 bridging-mode isolated-tunnel
 ip igmp snooping
 ip igmp snooping querier
radius nas-identifier test
radius nas-port-id 1
neighbor-info-interval 6
neighbor-inactivity-timeout 500
spanning-tree mst 2 priority 4096
spanning-tree errdisable recovery cause bpduguard
autoinstall configuration
--More--
nx9500-6C8809(config-profile-default-rfs4000)#

```

## Related Commands

|                              |                                               |
|------------------------------|-----------------------------------------------|
| <code>no</code> on page 1200 | Disables or reverts settings to their default |
|------------------------------|-----------------------------------------------|

### *traffic-class-mapping*

[Profile Config Commands](#) on page 862

Maps the IPv6 traffic class value of incoming IPv6 untagged packets to 802.1p priority. This mapping is required to provide priority of service to some packets over others. For example, VoIP packets get higher priority than data packets to provide a better quality of service for high priority voice traffic. Devices use the traffic class field in the IPv6 header to set this priority. This command allows you to assign a priority for different IPv6 traffic types.

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
traffic-class-mapping <IPv6-TRAFFIC-CLASS-VALUE> priority <0-7>
```

### Parameters

```
traffic-class-mapping <IPv6-TRAFFIC-CLASS-VALUE> priority <0-7>
```

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>traffic-class-mapping</b>            | Maps the IPv6 traffic class value of incoming IPv6 untagged packets to 802.1p priority                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>&lt;IPv6-TRAFFIC-CLASS-VALUE&gt;</b> | Specify the traffic class value of incoming IPv6 untagged packet(s) (could be a single value or a list. For example, 10-20, 25, 30-35). This is the DSCP 6-bit parameter in the header of every IP packet used for packet classification.                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>priority &lt;0-7&gt;</b>             | <p>Specify the 802.1p priority to map with the traffic-class value specified in the previous step</p> <ul style="list-style-type: none"><li>• &lt;0-7&gt; - Specify a value from 0 - 7.</li></ul> <p>The 802.1p priority is a 3-bit IP precedence value in the Type of Service field of the IP header used to set the priority. The valid values for this field are 0-7. Up to 64 entries are permitted. The priority values are:</p> <ul style="list-style-type: none"><li>• 0 - Best Effort</li><li>• 1 - Background</li><li>• 2 - Spare</li><li>• 3 - Excellent Effort</li><li>• 4 - Controlled Load</li><li>• 5 - Video</li><li>• 6 - Voice</li><li>• 7 - Network Control</li></ul> |

## Example

```
rfs4000-229D58(config-profile-TestRFS4000)#traffic-class-mapping 25 priority 2

rfs4000-229D58(config-profile-TestRFS4000)#show context
profile rfs4000 TestRFS4000
 traffic-class-mapping 25 priority 2
 no autoinstall configuration
 no autoinstall firmware
 crypto ikev1 policy ikev1-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 crypto remote-vpn-client
-More-
rfs4000-229D58(config-profile-TestRFS4000)#
```

## Related Commands

|                              |                                                                                                          |
|------------------------------|----------------------------------------------------------------------------------------------------------|
| <code>no</code> on page 1200 | Removes mapping between IPv6 traffic class value (of incoming IPv6 untagged packets) and 802.lp priority |
|------------------------------|----------------------------------------------------------------------------------------------------------|

### *traffic-shape*

[Profile Config Commands](#) on page 862

Enables traffic shaping and configures traffic shaping parameters. This command is applicable to both the profile and device configuration modes.

Traffic shaping is a means of regulating data transfers and ensuring a specific level of performance within a network. Traffic shaping does the following:

- Controls flow of packets based on their priority value. Prioritized traffic streams are given priority over less important traffic.
- Controls traffic on an interface to match its flow to the speed of a remote target's interface and ensure traffic conforms to applied policies
- Shapes traffic to meet downstream requirements and eliminate network congestion when data rates are in conflict.

Use this option to apply traffic shaping to specific applications or application categories. Note, in scenarios where a traffic class is matched against an application, application-category, and ACL rule, the application rule will be applied first, followed by the application-category, and finally the ACL. Further, using traffic shaping, an application takes precedence over an application category.

To enable traffic shaping, configure QoS values on the basis of which priority of service is provided to some packets over others. For example, VoIP packets get higher priority than data packets to provide a better quality of service for high priority voice traffic. For configuring IPv6 traffic class mappings, see [traffic-class-mapping](#) on page 1223. And for configuring DSCP traffic class mappings, see [dscp-mapping](#) on page 989.

---

**Supported in the following platforms:**

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530

**Syntax**

```
traffic-shape [activation-criteria|app-category|application|class|enable|priority-map|total-bandwidth]
```

```
traffic-shape activation-criteria [always|cluster-master|rf-domain-manager|vrrp-master <1-255>]
```

```
traffic-shape app-category <APP-CATEGORY-NAME> class <1-4>
```

```
traffic-shape application <APPLICATION-NAME> class <1-4>
```

```
traffic-shape class <1-4> [max-buffers|max-latency|rate]
```

```
traffic-shape class <1-4> max-buffers <1-400> {red-level <1-400>/red-percent <1-100>}
```

```
traffic-shape class <1-4> max-latency <1-1000000> [msec|usec]
```

```
traffic-shape class <1-4> rate [<1-250000> [Kbps|Mbps]]|total-bandwidth-percent <1-100>]
```

**Note**

The available range for the 'rate' field will vary depending on the unit selected. It is 250 - 250000 for Kbps and 1 - 250 for Mbps.

---

```
traffic-shape priority-map <0-7>
```

```
traffic-shape total-bandwidth <1-1000000> [Kbps|Mbps]
```

**Note**

The available range for the 'total-bandwidth' field will vary depending on the unit selected. It is 250 - 1000000 for Kbps and 1 - 1000 for Mbps.

---

```
traffic-shape enable
```

**Parameters**

```
traffic-shape activation-criteria [always|cluster-master|rf-domain-manager|vrrp-master <1-255>]
```

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>traffic-shape activation-criteria</b> | Configures traffic-shape activation criteria that determines when the device invokes traffic shaping                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>always</b>                            | Always invokes traffic shaping. This is the default setting.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>cluster-master</b>                    | Invokes traffic shaping when the device is the cluster master. The solitary cluster master (elected using a priority assignment scheme) is a cluster member that provides management configuration and Smart RF data to other members within the cluster. Cluster requests go through the elected master before dissemination to other cluster members.                                                                                                                                       |
| <b>rf-domain-manager</b>                 | Invokes traffic shaping when the device is the RF Domain manager. The RF Domain manager is the elected member capable of storing and provisioning configuration and firmware images for other members of the RF Domain.                                                                                                                                                                                                                                                                       |
| <b>vrrp-master &lt;1-255&gt;</b>         | Invokes traffic shaping when the device is the VRRP master. As the VRRP master, the device responds to ARP requests, forwards packets with a destination link MAC layer address equal to the virtual router MAC layer address, rejects packets addressed to the IP associated with the virtual router and accepts packets addressed to the IP associated with the virtual router. <ul style="list-style-type: none"> <li>• &lt;1-255&gt; - Specify the VRRP group ID from 1 - 255.</li> </ul> |

```
traffic-shape app-category <APP-CATEGORY-NAME> class <1-4>
```

|                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>traffic-shape app-category &lt;APP-CATEGORY-NAME&gt; class &lt;1-4&gt;</b> | Configures an application category to traffic-class mapping. Use this option to apply an application category to traffic-shaper class mapping. Naming and categorizing applications that do not fall into existing groups is an additional means of filtering and potentially limiting network airtime to consumptive non required applications negatively impacting network performance. <ul style="list-style-type: none"> <li>• class &lt;1-4&gt; - Map the specified application category to a traffic-shaper class from 1 - 4.</li> </ul> <p><b>Note:</b> app-category &lt;APP-CATEGORY-NAME&gt; - Specify the application category name. To list the available application categories, press [TAB] after entering app-category. Select the required category from the displayed list.</p> <p>Before configuring an application category to class mapping, ensure that the specified classes have been configured. Use the 'class &gt; [max-buffers max-latency rate]' option available with this command to configure a traffic shaper class. For more information, see following parameter tables.</p> |
|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
traffic-shape application <APPLICATION-NAME> class <1-4>
```

|                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>traffic-shape app-category &lt;APPLICATION-NAME&gt; class &lt;1-4&gt;</b> | Configures an application to traffic-class mapping. Use this option to apply an application to traffic-shaper class mapping. <ul style="list-style-type: none"> <li>• app-category &lt;APPLICATION-NAME&gt; - Specify the application name.</li> <li>• class &lt;1-4&gt; - Map the specified application to a traffic-shaper class from 1 - 4.</li> </ul> <p><b>Note:</b> Before configuring an application to class mapping, ensure that the specified classes have been configured. Use the 'class &gt; [max-buffers max-latency rate]' option available with this command to configure a traffic shaper class. For more information, see following tables.</p> |
|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
traffic-shape class <1-4> max-buffers <1-400> {red-level <1-400>|red-percent <1-100>}
```

|                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>traffic-shape class &lt;1-4&gt; max-buffers &lt;1-400&gt;</b> | <p>Configures the queue length limit for different traffic-shaper class</p> <ul style="list-style-type: none"> <li>class &lt;1-4&gt; – Specify the traffic-shaper class from 1 - 4.</li> <li>max-buffers &lt;1-400&gt; – Configures the maximum queue lengths for packets of different priority queues, after which the queue starts to drop packets. <ul style="list-style-type: none"> <li>&lt;1-400&gt; – Configure the queue length limit from 1 - 400 for packets of priority queues 0, 1, 2, 3, 4, 5, 6, and 7.</li> </ul> </li> </ul> <p><b>Note:</b> For access points the upper queue length limit is 400.</p>                                                                                                                                                               |
| <b>red-level &lt;1-400&gt;</b>                                   | <p>Optional. Performs Random Early Drop (RED) when a specified queue length in packets is reached</p> <ul style="list-style-type: none"> <li>&lt;1-400&gt; – Configure the queue length limit from 1 - 400 for packets of priority queues 0, 1, 2, 3, 4, 5, 6, and 7.</li> </ul> <p>The RED algorithm is a queuing technique for congestion avoidance. RED monitors the average queue size and drops or marks packets. If the buffer is near empty, all incoming packets are accepted. When the queue grows, the probability for dropping an incoming packet also grows. When the buffer is full, the probability has reached 1 and all incoming packets are dropped.</p> <p><b>Note:</b> For more information on default values, see the Usage Guidelines section in this topic.</p> |
| <b>red-percent &lt;1-100&gt;</b>                                 | <p>Optional. Performs RED when a specified value, which is a percentage of the max-buffers configured, is reached</p> <ul style="list-style-type: none"> <li>&lt;1-100&gt; – Configure the percentage of the maxi-buffers from 1 - 100 for packets of priority queues 0, 1, 2, 3, 4, 5, 6, and 7.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

```
traffic-shape class <1-4> max-latency <1-1000000> [msec|usec]
```

|                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>traffic-shape class &lt;1-4&gt; max-latency &lt;1-1000000&gt; [msec  usec]</b> | <p>Configures the max-latency for different traffic-shaper class. Max latency specifies the time limit after which packets start dropping (maximum packet delay in the queue). The maximum number of entries is 8.</p> <ul style="list-style-type: none"> <li>class &lt;1-4&gt; – Specify the traffic-shaper class from 1 - 4.</li> <li>max-latency &lt;1-1000000&gt; – Configures the max-latency for packets of different priority queues, after which the queue starts to drop packets. <ul style="list-style-type: none"> <li>&lt;1-1000000&gt; – Configure the max-latency from 1 - 100000 for packets of priority queues 0, 1, 2, 3, 4, 5, 6, and 7.</li> </ul> </li> </ul> <p>[msec usec] – Configures the unit for measuring latency as milliseconds (msec) or microseconds (usec). The default setting is msec.</p> |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
traffic-shape class <1-4> rate [<1-250000> [Kbps|Mbps]|total-bandwidth-percent <1-100>]
```

|                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>traffic-shape class &lt;1-4&gt; rate</b>  | <p>Configures traffic rate, in either Kbps, Mbps or percentage, for the different traffic shaper class. Specify rates for different traffic shaper class to control the maximum traffic rate sent or received on an interface. Consider this form of rate limiting on interfaces at the edge of a network to limit traffic into or out of the network. Traffic within the set limit is sent and traffic exceeding the set limit is dropped or sent with a different priority.</p> <ul style="list-style-type: none"> <li>class &lt;1-4&gt; – Specify the traffic-shaper class from 1 - 4.</li> </ul> |
| <b>&lt;1-250000&gt; [Kbps   Mbps]</b>        | <p>Configures the traffic rate, in Kbps, Mbps, for the class specified in the previous step</p> <ul style="list-style-type: none"> <li>&lt;1-250000&gt; – Specify the rate from 1 - 250000.</li> <li>[Kbps Mbps] – Configures the unit for measuring bandwidth as Kbps or Mbps. The default setting is Kbps.</li> </ul> <p><b>Note:</b> The range varies depending on the unit selected. It is 1 - 250 Mbps, or 250 - 250000 Kbps.</p>                                                                                                                                                               |
| <b>total-bandwidth-percent &lt;1-100&gt;</b> | <p>Configures the traffic rate, as a percentage of the total available bandwidth, for the class specified in the previous first step</p> <ul style="list-style-type: none"> <li>&lt;1-100&gt; – Specify the traffic rate from 1 - 100% of the total bandwidth.</li> </ul>                                                                                                                                                                                                                                                                                                                            |

traffic-shape priority-map <0-7>

|                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>traffic-shape priority-map &lt;0-7&gt;</b> | <p>Configures the traffic-shaper queues, within a class, having different priority values (0, 1, 2, 3, 4, 5, 6, and 7). There are 8 queues (0 - 7), and traffic is queued in each based on the incoming packet's 802.1p 3-bit priority markings.</p> <ul style="list-style-type: none"> <li>priority-map &lt;0-7&gt; – Specify the priority from 0 - 7 for priority levels 0, 1, 2, 3, 4, 5, 6, and 7.</li> </ul> <p>The IEEE 802.1p standards sets a 3-bit value in the MAC header to indicate prioritization. This 3-bit value provides priority levels ranging from 0 to 7 (i.e., a total of 8 levels), with level 7 representing the highest priority. This permits packets to cluster and form different traffic classes. In case of network congestion, packets with higher priority receive preferential treatment while low priority packets are kept on hold.</p> |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

traffic-shape total-bandwidth <1-1000000> [Kbps | Mbps]

|                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>traffic-shape total-bandwidth &lt;1-1000000&gt; [Kbps   Mbps]</b> | <p>Configures the total-bandwidth for traffic shaping</p> <ul style="list-style-type: none"> <li>&lt;1-1000000&gt; – Specify the value from 1 - 1000000 Kbps/Mbps. The default value is 10 Mbps.</li> <li>[Kbps Mbps] – Configures the unit for measuring bandwidth as Kbps or Mbps. The default setting is Mbps.</li> </ul> <p><b>Note:</b> The range varies depending on the unit selected. It is 1 - 1000 Mbps, or 250 - 1000000 Kbps.</p> |
|----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

traffic-shape enable

|                             |                                                                                                                                                                               |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>traffic-shape enable</b> | <p>Enables traffic shaping using the defined bandwidth, rate and class mappings configured using this command</p> <p><b>Note:</b> Traffic shaping is disabled by default.</p> |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Usage Guidelines

Following are the default max-buffers set for the traffic shaper classes:



```
traffic-shape class 1 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23 25 20 15 10
traffic-shape class 2 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23 25 20 15 10
traffic-shape class 3 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23 25 20 15 10
traffic-shape class 4 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23 25 20 15 10
```

Following is the default priority-map settings:

```
traffic-shape priority-map 2 0 1 3 4 5 6 7
```

### Example

```
nx9500-6C8809(config-profile-ProfileNX5500)#show context include-factory | include traffic-
shape
 traffic-shape priority-map 2 0 1 3 4 5 6 7
 traffic-shape class 1 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23 25 20 15
 10
 traffic-shape class 2 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23 25 20 15
 10
 traffic-shape class 3 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23 25 20 15
 10
 traffic-shape class 4 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23 25 20 15
 10
 traffic-shape activation-criteria always
 traffic-shape total-bandwidth 10 Mbps
 no traffic-shape enable
nx9500-6C8809(config-profile-ProfileNX5500)#

nx9500-6C8809(config-profile-ProfileNX5500)#traffic-shape enable
nx9500-6C8809(config-profile-ProfileNX5500)#traffic-shape class 1 rate 250 Mbps
nx9500-6C8809(config-profile-ProfileNX5500)#traffic-shape application Bing class 1
nx9500-6C8809(config-profile-ProfileNX5500)#traffic-shape total-bandwidth 200 Mbps

nx9500-6C8809(config-profile-ProfileNX5500)#show context include-factory | include traffic-
shape
 traffic-shape priority-map 2 0 1 3 4 5 6 7
 traffic-shape class 1 rate 250 Mbps
 traffic-shape class 1 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23 25 20 15
 10
 traffic-shape class 2 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23 25 20 15
 10
 traffic-shape class 3 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23 25 20 15
 10
 traffic-shape class 4 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23 25 20 15
 10
 traffic-shape activation-criteria always
 traffic-shape application Bing class 1
 traffic-shape total-bandwidth 200 Mbps
 traffic-shape enable
nx9500-6C8809(config-profile-ProfileNX5500)#
```

### Related Commands

|                              |                                                                             |
|------------------------------|-----------------------------------------------------------------------------|
| <code>no</code> on page 1200 | Removes traffic shaping configuration or reverts them to the default values |
|------------------------------|-----------------------------------------------------------------------------|

*trustpoint* (profile-config-mode)

[Profile Config Commands](#) on page 862

Configures the trustpoint assigned for validating a CMP auth Operator

A certificate links identity information with a public key enclosed in the certificate.

A CA is a network authority that issues and manages security credentials and public keys for message encryption. The CA signs all digital certificates it issues with its own private key. The corresponding public key is contained within the certificate and is called a CA certificate. A browser must contain the CA certificate in its Trusted Root Library so it can trust certificates signed by the CA's private key.

Depending on the public key infrastructure, the digital certificate includes the owner's public key, the certificate expiration date, the owner's name and other public key owner information.

Each certificate is digitally signed by a trustpoint. The trustpoint signing the certificate can be a certificate authority, corporation or individual. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters, and an association with an enrolled identity certificate.



#### Note

Certificates/trustpoints used in this command should be verifiable as existing on the device. For information on configuring trustpoints on a device, see [trustpoint \(device-config-mode\)](#) on page 1282.

#### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
trustpoint [cmp-auth-operator|https|radius-ca|radius-server] <TRUSTPOINT-NAME>
```

#### Parameters

```
trustpoint [cmp-auth-operator|https|radius-ca|radius-server] <TRUSTPOINT-NAME>
```

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>trustpoint</b>        | Assigns an existing trustpoint to validate CMP auth operator, client certificates, and RADIUS server certificate                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>https</b>             | Assigns an existing trustpoint to validate HTTPS requests                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>cmp-auth-operator</b> | Assigns an existing trustpoint to validate CMP auth operator Once validated, CMP is used to obtain and manage digital certificates in a PKI network. Digital certificates link identity information with a public key enclosed within the certificate, and are issued by the CA. Use this command to specify the CMP-assigned trustpoint. When specified, devices send a certificate request to the CMP supported CA server, and download the certificate directly from the CA server. CMP supports multiple request options through for device communicating to a CMP supported CA server. The device can initiate a request for getting the certificates from the server. It can also auto update the certificates which are about to expire. |
| <b>radius-ca</b>         | Assigns an existing trustpoint to validate client certificates in EAP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

|                                |                                                                                                                                                                                                                                                                   |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>radius-server</b>           | Assigns an existing trustpoint to validate RADIUS server certificate                                                                                                                                                                                              |
| <b>&lt;TRUSTPOINT-NAME&gt;</b> | The following keyword is common to all of the above parameters: <ul style="list-style-type: none"> <li>• &lt;TRUSTPOINT-NAME&gt; – After selecting the service to validate, specify the trustpoint name (should be existing and stored on the device).</li> </ul> |

### Example

```
nx9500-6C8809(config-profile-testNX9500)#trustpoint cmp-auth-operator test
```

```
nx9500-6C8809(config-profile-testNX9500)#show context
profile nx9000 testNX9500
 no autoinstall configuration
 no autoinstall firmware
 crypto ikev1 policy ikev1-default
 isakmp-proposal default encryption aes-256 group 2 hash sha

 service pm sys-restart
 router bgp
 trustpoint cmp-auth-operator test
nx9500-6C8809(config-profile-testNX9500)#
```

### Related Commands

|                        |                                           |
|------------------------|-------------------------------------------|
| <b>no</b> on page 1200 | Removes trustpoint-related configurations |
|------------------------|-------------------------------------------|

## tunnel-controller

[Profile Config Commands](#) on page 862

Configures the tunneled WLAN (extended VLAN) wireless controller or service platform's name

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
tunnel-controller <NAME>
```

### Parameters

```
tunnel-controller <NAME>
```

|                                                 |                                                                                                                                                                                  |
|-------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>tunnel-controller</b><br><b>&lt;NAME&gt;</b> | Configures the tunneled WLAN (extended VLAN) wireless controller or service platform's name <ul style="list-style-type: none"> <li>• &lt;NAME&gt; – Specify the name.</li> </ul> |
|-------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Example

```
rfs7000-37FABE(config-profile-default-rfs4000)#tunnel-controller testgroup
```

## Related Commands

|                              |                                                                                                         |
|------------------------------|---------------------------------------------------------------------------------------------------------|
| <code>no</code> on page 1200 | Removes the configured the tunneled WLAN (extended VLAN) wireless controller or service platform's name |
|------------------------------|---------------------------------------------------------------------------------------------------------|

*use*

[Profile Config Commands](#) on page 862

Associates existing policies with this profile. This command is also applicable to the device configuration mode.

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax Profiles Mode

```
use [auto-provisioning-policy|bonjour-gw-forwarding-policy|bonjour-gw-query-forwarding-policy|captive-portal|client-identity-group|crypto-cmp-policy| database-client-policy|dhcp-server-policy|dhcpv6-server-policy| event-system-policy|firewall-policy|global-association-list|guest-management|ip-access-list|ipv6-access-list|iot-device-type-imagotag-policy|location-policy|management-policy| radius-server-policy|role-policy|routing-policy|web-filter-policy] <POLICY-NAME>
```

```
use ip/ipv6-access-list <IP/IPV6-ACL-NAME> traffic-shape class <1-4>
```

### Syntax Device Mode

```
use [auto-provisioning-policy|bonjour-gw-forwarding-policy|bonjour-gw-query-forwarding-policy|captive-portal|client-identity-group|crypto-cmp-policy| database-client-policy|database-policy|dhcp-server-policy|dhcpv6-server-policy| enterprise-ui|event-system-policy|firewall-policy|global-association-list| guest-management|iot-device-type-imagotag-policy|ip-access-list|ipv6-access-list|license|location-policy| management-policy| nsight-policy|profile|radius-server-policy|rf-domain| role-policy| routing-policy|rtl-server-policy|sensor-policy|web-filter-policy| wips-policy] <POLICY-NAME>
```



#### Note

The following tables contain the 'use' command parameters for the Profile and Device configuration modes.

### Parameters Profiles Mode

```
use [auto-provisioning-policy|bonjour-gw-forwarding-policy| bonjour-gw-query-forwarding-policy|captive-portal|client-identity-group|crypto-cmp-policy|
```

database-client-policy|dhcp-server-policy|dhcpv6-server-policy|event-system-policy|  
 firewall-policy|global-association-list|guest-management|iot-device-type-imagotag-policy|  
 ip-access-list|ipv6-access-list|management-policy|radius-server-policy|role-policy|  
 routing-policy|web-filter-policy] <POLICY-NAME>

|                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>use</b>                                                               | Associates the specified policies with this profile<br>The specified policies should be existing and configured.                                                                                                                                                                                                                                                                                   |
| <b>auto-provisioning-policy &lt;POLICY-NAME&gt;</b>                      | Associates an auto provisioning policy <ul style="list-style-type: none"> <li>• &lt;POLICY-NAME&gt; - Specify the auto provisioning policy name.</li> </ul>                                                                                                                                                                                                                                        |
| <b>bonjour-gw-forwarding-policy &lt;POLICY-NAME&gt;</b>                  | Uses an existing Bonjour GW Forwarding policy with a profile or device <ul style="list-style-type: none"> <li>• &lt;POLICY-NAME&gt; - Specify the Bonjour GW Forwarding policy name (should be existing and configured).</li> </ul> <p>For more information on Bonjour GW Forwarding policy, see <a href="#">bonjour-gw-forwarding-policy</a> on page 291.</p>                                     |
| <b>bonjour-gw-query-forwarding-policy &lt;POLICY-NAME&gt;</b>            | Uses an existing Bonjour GW Query Forwarding policy with a profile or device <ul style="list-style-type: none"> <li>• &lt;POLICY-NAME&gt; - Specify the Bonjour GW Query Forwarding policy name (should be existing and configured).</li> </ul>                                                                                                                                                    |
| <b>captive-portal-server &lt;CAPTIVE-PORTAL&gt;</b>                      | Configures access to a specified captive portal with this profile <ul style="list-style-type: none"> <li>• &lt;CAPTIVE-PORTAL&gt; - Specify the captive portal name.</li> </ul>                                                                                                                                                                                                                    |
| <b>client-identity-identity-group &lt;CLIENT-IDENTITY-GROUP-NAME&gt;</b> | Associates an existing client identity group with this profile <ul style="list-style-type: none"> <li>• &lt;CLIENT-IDENTITY-GROUP-NAME&gt; - Specify the client identity group name.</li> </ul> <p>For more information on the 'client-identity' and 'client-identity-group' commands, see <a href="#">client-identity</a> on page 336 and <a href="#">client-identity-group</a> on page 343.</p>  |
| <b>crypto-cmp-policy &lt;POLICY-NAME&gt;</b>                             | Associates an existing crypto certificate management protocol (CMP) policy with this profile <ul style="list-style-type: none"> <li>• &lt;POLICY-NAME&gt; - Specify the CMP policy name.</li> </ul> <p>For more information on configuring a crypto CMP policy, see <a href="#">CRYPTO-CMP-POLICY</a> on page 1831.</p>                                                                            |
| <b>database-client-policy &lt;POLICY-NAME&gt;</b>                        | Associates an existing database client policy with a profile <ul style="list-style-type: none"> <li>• &lt;POLICY-NAME&gt; - Specify the policy name (should be existing and configured).</li> </ul> <p>For more information on database client policy, see <a href="#">database-client-policy global-config</a> on page 359.<br/>Applicable only to the VX9000 model virtual machine platform.</p> |
| <b>dhcp-server-policy &lt;DHCP-POLICY&gt;</b>                            | Associates a DHCP server policy <ul style="list-style-type: none"> <li>• &lt;DHCP-POLICY&gt; - Specify the DHCP server policy name.</li> </ul>                                                                                                                                                                                                                                                     |
| <b>dhcpv6-server-policy &lt;DHCPv6-POLICY&gt;</b>                        | Associates a DHCPv6 server policy <ul style="list-style-type: none"> <li>• &lt;DHCPv6-POLICY&gt; - Specify the DHCPv6 server policy name.</li> </ul>                                                                                                                                                                                                                                               |

|                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>event-system-policy &lt;EVENT-SYSTEM-POLICY&gt;</b>                              | <p>Associates an event system policy</p> <ul style="list-style-type: none"> <li>• &lt;EVENT-SYSTEM-POLICY&gt; – Specify the event system policy name.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>firewall-policy &lt;FW-POLICY&gt;</b>                                            | <p>Associates a firewall policy</p> <ul style="list-style-type: none"> <li>• &lt;FW-POLICY&gt; – Specify the firewall policy name.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>global-association-list server &lt;GLOBAL-ASSOC-LIST-NAME&gt;</b>                | <p>Associates the specified global association list with the controller profile</p> <ul style="list-style-type: none"> <li>• &lt;GLOBAL-ASSOC-LIST-NAME&gt; – Specify the global association list name.</li> </ul> <p>Once associated, the controller, using this profile, applies this association list to requests received from all adopted APs. For more information on global association list, see <a href="#">global-association-list</a> on page 428.</p>                                                                                                                                                             |
| <b>guest-management &lt;GUEST-MANAGEMENT-POLICY-NAME&gt;</b>                        | <p>Associates the specified guest management policy with the controller profile</p> <ul style="list-style-type: none"> <li>• &lt;GUEST-MANAGEMENT-POLICY-NAME&gt; – Specify the guest management policy name (should be existing and configured).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                  |
| <b>iot-device-type-imagotag-policy &lt;POLICY-NAME&gt;</b>                          | <p>Associates an IoT Imago Tag policy to an AP's profile or device context.</p> <ul style="list-style-type: none"> <li>• &lt;POLICY-NAME&gt; – Specify the policy name. When associated, the policy enables support for SES-imagotag's ESL (Electronic Shelf Label) tags and communicator on WING APs with USB interfaces. This feature is supported only on AP 8432 model access points.</li> </ul>                                                                                                                                                                                                                          |
| <b>ip/ipv6-access-list &lt;IP/IPv6-ACL-NAME&gt; traffic-shape class &lt;1-4&gt;</b> | <p>Associates an IP and/or IPv6 ACL with this profile and applies it as a firewall for the selected traffic-shape class</p> <ul style="list-style-type: none"> <li>• &lt;IP/IPv6-ACL-NAME&gt; – Specify the IP/IPv6 ACL name (should be existing and configured)</li> <li>• traffic-shape class &lt;1-4&gt; – Selects the traffic-shape class to apply the above specified IP/IPv6 ACL</li> </ul> <p>&lt;1-4&gt; – Select the traffic-shape class from 1 - 4.</p>                                                                                                                                                             |
| <b>location-policy &lt;POLICY-NAME&gt;</b>                                          | <p>Associates a location policy to the device profile. The Location policy is a means to upload site hierarchy to the ExtremeLocation server through the WING controller (NOC, standalone APs, virtual controllers). The location policy points to the ExtremeLocation server and provides the Tenant authentication key needed to authenticate with the server.</p> <p>It is applicable to the following platform profiles: AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8432, AP 8533.</p> <ul style="list-style-type: none"> <li>• &lt;POLICY-NAME&gt; – Specify the policy name.</li> </ul> |
| <b>management-policy &lt;MNGT-POLICY&gt;</b>                                        | <p>Associates a management policy</p> <ul style="list-style-type: none"> <li>• &lt;MNGT-POLICY&gt; – Specify the management policy name.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>radius-server-policy &lt;RADIUS-POLICY&gt;</b>                                   | <p>Associates a device onboard RADIUS policy</p> <ul style="list-style-type: none"> <li>• &lt;RADIUS-POLICY&gt; – Specify the RADIUS policy name.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>role-policy &lt;ROLE-POLICY&gt;</b>                                              | <p>Associates a role policy</p> <ul style="list-style-type: none"> <li>• &lt;ROLE-POLICY&gt; – Specify the role policy name.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

|                                                        |                                                                                                                                                                      |
|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>routing-policy</b><br><b>&lt;ROUTING-POLICY&gt;</b> | Associates a routing policy <ul style="list-style-type: none"> <li>• &lt;ROUTING-POLICY&gt; – Specify the routing policy name.</li> </ul>                            |
| <b>web-filter-policy</b><br><b>&lt;POLICY-NAME&gt;</b> | Associates an existing Web Filter policy with a profile or device <ul style="list-style-type: none"> <li>• &lt;POLICY-NAME&gt; – Specify the policy name.</li> </ul> |

### Parameters Device Mode

use [auto-provisioning-policy|bonjour-gw-forwarding-policy|  
bonjour-gw-query-forwarding-policy|captive-portal|client-identity-group|crypto-cmp-policy|  
database-client-policy|database-policy|dhcp-server-policy|dhcpv6-server-policy|  
enterprise-ui|event-system-policy|firewall-policy|global-association-list|guest-management|  
iot-device-type-imagotag-policy|ip-access-list|ipv6-access-list|license|location-policy|  
management-policy|nsight-policy|profile|radius-server-policy|rf-domain|role-policy|  
routing-policy|rtl-server-policy|sensor-policy|wips-policy|smart-rf-policy|web-filter-  
policy]  
<POLICY-NAME>

|                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>use</b>                                                                         | Associates the following policies with this device:                                                                                                                                                                                                                                                                                                                                              |
| <b>auto-provisioning-policy</b><br><b>&lt;POLICY-NAME&gt;</b>                      | Associates an auto provisioning policy <ul style="list-style-type: none"> <li>• &lt;POLICY-NAME&gt; – Specify the auto provisioning policy name.</li> </ul>                                                                                                                                                                                                                                      |
| <b>bonjour-gw-forwarding-policy</b><br><b>&lt;POLICY-NAME&gt;</b>                  | Uses an existing Bonjour GW Forwarding policy with a profile or device <ul style="list-style-type: none"> <li>• &lt;POLICY-NAME&gt; – Specify the Bonjour GW Forwarding policy name (should be existing and configured).</li> </ul> <p>For more information on Bonjour GW Forwarding policy, see <a href="#">bonjour-gw-forwarding-policy</a> on page 291.</p>                                   |
| <b>bonjour-gw-query-forwarding-policy</b><br><b>&lt;POLICY-NAME&gt;</b>            | Uses an existing Bonjour GW Query Forwarding policy with a profile or device <ul style="list-style-type: none"> <li>• &lt;POLICY-NAME&gt; – Specify the Bonjour GW Query Forwarding policy name (should be existing and configured).</li> </ul>                                                                                                                                                  |
| <b>captive-portal-server</b><br><b>&lt;CAPTIVE-PORTAL&gt;</b>                      | Configures access to a specified captive portal <ul style="list-style-type: none"> <li>• &lt;CAPTIVE-PORTAL&gt; – Specify the captive portal name.</li> </ul>                                                                                                                                                                                                                                    |
| <b>client-identity-identity-group</b><br><b>&lt;CLIENT-IDENTITY-GROUP-NAME&gt;</b> | Associates an existing client identity group with this device <ul style="list-style-type: none"> <li>• &lt;CLIENT-IDENTITY-GROUP-NAME&gt; – Specify the client identity group name.</li> </ul> <p>For more information on the 'client-identity' and 'client-identity-group' commands, see <a href="#">client-identity</a> on page 336 and <a href="#">client-identity-group</a> on page 343.</p> |
| <b>crypto-cmp-policy</b><br><b>&lt;POLICY-NAME&gt;</b>                             | Associates an existing crypto certificate management protocol (CMP) policy <ul style="list-style-type: none"> <li>• &lt;POLICY-NAME&gt; – Specify the CMP policy name.</li> </ul> <p>For more information on configuring a crypto CMP policy, see <a href="#">CRYPTO-CMP-POLICY</a> on page 1831.</p>                                                                                            |

|                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>database-client-policy</b><br><b>&lt;POLICY-NAME&gt;</b>                                                       | <p>Associates an existing database client policy with a device</p> <ul style="list-style-type: none"> <li>• &lt;POLICY-NAME&gt; – Specify the policy name (should be existing and configured).</li> </ul> <p>For more information on database client policy, see <a href="#">database-client-policy global-config</a> on page 359.</p> <p>Applicable only to the NX 95XX and VX 9000 model service platforms.</p>                                                                                                                                                                       |
| <b>database-policy</b><br><b>&lt;DATABASE-POLICY-NAME&gt;</b>                                                     | <p>Associates an existing database policy with this device</p> <ul style="list-style-type: none"> <li>• &lt;DATABASE-POLICY-NAME&gt; – Specify the database policy name.</li> </ul> <p><b>Note:</b> For more information on configuring a database policy, see <a href="#">database-policy global config</a> on page 363.</p>                                                                                                                                                                                                                                                           |
| <b>dhcp-server-policy</b><br><b>&lt;DHCP-POLICY&gt;</b>                                                           | <p>Associates a DHCP server policy</p> <ul style="list-style-type: none"> <li>• &lt;DHCP-POLICY&gt; – Specify the DHCP server policy name.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>dhcpv6-server-policy</b><br><b>&lt;DHCPv6-POLICY&gt;</b>                                                       | <p>Associates a DHCPv6 server policy</p> <ul style="list-style-type: none"> <li>• &lt;DHCPv6-POLICY&gt; – Specify the DHCPv6 server policy name.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>enterprise-ui</b>                                                                                              | <p>Enables application of the site controller’s Enterprise user interface (UI) on all management points (controllers and access points)</p> <p>For example, the site controller is NX5500 and an AP7562 is adopted to it. To enable the access point to also use the Enterprise UI:</p> <p>On the AP7562’s profile configuration mode execute: use &gt; enterprise-ui</p> <p>On adoption and application of this profile, the AP7562 access point resets and reboots using the Enterprise UI. Once using the Enterprise UI, on all subsequent adoptions, the AP does not get reset.</p> |
| <b>event-system-policy</b><br><b>&lt;EVENT-SYSTEM-POLICY&gt;</b>                                                  | <p>Associates an event system policy</p> <ul style="list-style-type: none"> <li>• &lt;EVENT-SYSTEM-POLICY&gt; – Specify the event system policy name.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>firewall-policy</b><br><b>&lt;FW-POLICY&gt;</b>                                                                | <p>Associates a firewall policy</p> <ul style="list-style-type: none"> <li>• &lt;FW-POLICY&gt; – Specify the firewall policy name.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>global-association-list server</b><br><b>&lt;GLOBAL-ASSOC-LIST-NAME&gt;</b>                                    | <p>Associates the specified global association list with the device (controller)</p> <ul style="list-style-type: none"> <li>• &lt;GLOBAL-ASSOC-LIST-NAME&gt; – Specify the global association list name.</li> </ul> <p>Once associated, the controller applies this association list to requests received from all adopted APs. For more information on global association list, see <a href="#">global-association-list</a> on page 428.</p>                                                                                                                                           |
| <b>guest-management</b><br><b>&lt;GUEST-MANAGEMENT-POLICY-NAME&gt;</b>                                            | <p>Associates the specified guest management policy with this device</p> <ul style="list-style-type: none"> <li>• &lt;GUEST-MANAGEMENT-POLICY-NAME&gt; – Specify the guest management policy name (should be existing and configured).</li> </ul>                                                                                                                                                                                                                                                                                                                                       |
| <b>ip/ipv6-access-list</b><br><b>&lt;IP/IPv6-ACL-NAME&gt;</b><br><b>traffic-shape class</b><br><b>&lt;1-4&gt;</b> | <p>Associates an IP and/or IPv6 ACL with this device and applies it as a firewall for a selected traffic-shape class</p> <ul style="list-style-type: none"> <li>• &lt;IP/IPv6-ACL-NAME&gt; – Specify the IP/IPv6 ACL name (should be existing and configured)</li> <li>• traffic-shape class &lt;1-4&gt; – Selects the traffic-shape class to apply the above specified IP/IPv6 ACL</li> <li>• &lt;1-4&gt; – Select the traffic-shape class from 1 - 4.</li> </ul>                                                                                                                      |



|                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>license &lt;WORD&gt;</b>                       | <p>Associates a Web filtering license with this device</p> <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Provide a 256 character maximum license string for the Web filtering feature. Web filtering is used to restrict access to specific resources on the Internet.</li> </ul>                                                                                                                                                                                                                                                                                                                                |
| <b>location-policy &lt;POLICY-NAME&gt;</b>        | <p>Associates a location policy to the device self. The Location policy is a means to upload site hierarchy to the ExtremeLocation server through the WiNG controller (NOC, standalone APs, virtual controllers). The location policy points to the ExtremeLocation server and provides the Tenant authentication key needed to authenticate with the server.</p> <p>It is applicable to the following platform profiles: AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8432, AP 8533.</p> <ul style="list-style-type: none"> <li>• &lt;POLICY-NAME&gt; - Specify the policy name.</li> </ul> |
| <b>management-policy &lt;MNGT-POLICY&gt;</b>      | <p>Associates a management policy</p> <ul style="list-style-type: none"> <li>• &lt;MNGT-POLICY&gt; - Specify the management policy name.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>nsight-policy &lt;NSIGHT-POLICY-NAME&gt;</b>   | <p>Associates a specified NSight policy with this device</p> <ul style="list-style-type: none"> <li>• &lt;NSIGHT-POLICY-NAME&gt; - Specify the NSight policy name (should be existing and configured).</li> </ul> <p><b>Note:</b> Use this command to associate an NSight policy to a controller to enable it to function as the NSight server. For more information, see <a href="#">nsight-policy (global-config-mode)</a> on page 479.</p>                                                                                                                                                                              |
| <b>profile &lt;PROFILE-NAME&gt;</b>               | <p>Associates a profile with this device</p> <ul style="list-style-type: none"> <li>• &lt;PROFILE-NAME&gt; - Specify the profile name.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>radius-server-policy &lt;RADIUS-POLICY&gt;</b> | <p>Associates a device onboard RADIUS policy</p> <ul style="list-style-type: none"> <li>• &lt;RADIUS-POLICY&gt; - Specify the RADIUS policy name.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>rf-domain &lt;RF-DOMAIN-NAME&gt;</b>           | <p>Associates an RF Domain</p> <ul style="list-style-type: none"> <li>• &lt;RF-DOMAIN-NAME&gt; - Specify the RF Domain name.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>role-policy &lt;ROLE-POLICY&gt;</b>            | <p>Associates a role policy</p> <ul style="list-style-type: none"> <li>• &lt;ROLE-POLICY&gt; - Specify the role policy name.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>routing-policy &lt;ROUTING-POLICY&gt;</b>      | <p>Associates a routing policy</p> <ul style="list-style-type: none"> <li>• &lt;ROUTING-POLICY&gt; - Specify the routing policy name.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>rtl-server-policy &lt;POLICY-NAME&gt;</b>      | <p>Associates a Real Time Locationing (RTL) server policy with an access point. When associated, enables the access point to directly send RSSI feeds to the third-party Euclid RTL server.</p> <ul style="list-style-type: none"> <li>• &lt;POLICY-NAME&gt; - Specify the RTL server policy name (should be existing and configured).</li> </ul>                                                                                                                                                                                                                                                                          |
| <b>sensor-policy &lt;POLICY-NAME&gt;</b>          | <p>Associates a sensor policy with an access point or controller. When associated, WiNG controllers and access points function as sensors.</p> <ul style="list-style-type: none"> <li>• &lt;POLICY-NAME&gt; - Specify the sensor policy name (should be existing and configured).</li> </ul>                                                                                                                                                                                                                                                                                                                               |

|                                                        |                                                                                                                 |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| <b>wips-policy</b><br><b>&lt;WIPS-POLICY&gt;</b>       | Associates a WIPS policy<br>• <WIPS-POLICY> - Specify the WIPS policy name.                                     |
| <b>web-filter-policy</b><br><b>&lt;POLICY-NAME&gt;</b> | Associates an existing Web Filter policy with a profile or device<br>• <POLICY-NAME> - Specify the policy name. |

**Example**

```

nx9500-6C8809(config-profile-default-rfs4000)#use event-system-policy TestEventSysPolicy

nx9500-6C8809(config-profile-default-rfs4000)#show context
profile rfs4000 default-rfs4000
mint link ip 1.2.3.4
mint level 1 area-id 88
.....
interface ge3
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface ge4
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface pppoe1
use event-system-policy TestEventSysPolicy
use firewall-policy default
ntp server 172.16.10.10 prefer version 1
--More--
nx9500-6C8809(config-profile-default-rfs4000)#

```

**Related Commands**

|                        |                                                           |
|------------------------|-----------------------------------------------------------|
| <b>no</b> on page 1200 | Disassociates a specified policy from this profile/device |
|------------------------|-----------------------------------------------------------|

*vrrp*

[Profile Config Commands](#) on page 862

Configures VRRP group settings

A default gateway is a critical resource for connectivity. However, it is prone to a single point of failure. Thus, redundancy for the default gateway is required. If WAN backhaul is available, and a router failure occurs, then the controller should act as a router and forward traffic on to its WAN link.

Define an external VRRP configuration when router redundancy is required in a network requiring high availability.

Central to VRRP configuration is the election of a VRRP master. A VRRP master (once elected) performs the following functions:

- Responds to ARP requests
- Forwards packets with a destination link layer MAC address equal to the virtual router's MAC address

- Rejects packets addressed to the IP address associated with the virtual router, if it is not the IP address owner
- Accepts packets addressed to the IP address associated with the virtual router, if it is the IP address owner or accept mode is true.

The nodes that lose the election process enter a backup state. In the backup state they monitor the master for any failures, and in case of a failure one of the backups, in turn, becomes the master and assumes the management of the designated virtual IPs. A backup does not respond to an ARP request, and discards packets destined for a virtual IP resource.

#### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
vrrp [<1-255>|version]
```

```
vrrp <1-255> [delta-priority|description|interface|ip|monitor|preempt|priority| sync-group|timers]
```

```
vrrp <1-255> [delta-priority <1-253>|description <LINE>|ip <IP> {<IP>}|preempt {delay <1-65535>}|priority <1-254>|sync-group]
```

```
vrrp <1-255> interface vlan <1-4094>
```

```
vrrp <1-255> monitor [<IF-NAME>|critical-resource|pppoe1|vlan|wwan1]
```

```
vrrp <1-255> monitor [<IF-NAME>|pppoe1|vlan <1-4094>|wwan1] {(<IF-NAME>|critical-resource|pppoe1|vlan|wwan1)}
```

```
vrrp <1-255> monitor critical-resource <CRM-NAME1> <CRM-NAME2> <CRM-NAME3> <CRM-NAME4> (action [decrement-priority|increment-priority] {<IF-NAME>|pppoe1| vlan|wwan1})
```

```
vrrp <1-255> timers advertise [<1-255>|centiseconds <25-4095>|msec <250-999>]
```

```
vrrp version [2|3]
```

#### Parameters

```
vrrp <1-255> [delta-priority <1-253>|description <LINE>|vrrp ip <IP> {<IP>}| preempt {delay <1-65535>}|priority <1-254>|sync-group]
```

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vrrp &lt;1-255&gt;</b>              | Configures the virtual router ID from 1- 255. Identifies the virtual router the packet is reporting status for.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>delta-priority &lt;1-253&gt;</b>    | Configures the priority to decrement (local link monitoring and critical resource monitoring) or increment (critical resource monitoring). When the monitored interface is down, the configured priority decrements by a value defined by the delta-priority option. When monitoring critical resources, the value increments by the delta-priority option. <ul style="list-style-type: none"> <li>• &lt;1-253&gt; - Specify the delta priority level from 1- 253.</li> </ul>                                                                                      |
| <b>description &lt;LINE&gt;</b>        | Configures a text description for the virtual router to further distinguish it from other routers with similar configuration <ul style="list-style-type: none"> <li>• &lt;LINE&gt; - Provide a description (a string from 1- 64 characters in length)</li> </ul>                                                                                                                                                                                                                                                                                                   |
| <b>ip &lt;IP-ADDRESSES&gt;</b>         | Identifies the IP address(es) backed by the virtual router. These are IP addresses of Ethernet switches, routers, and security appliances defined as virtual router resources. <ul style="list-style-type: none"> <li>• &lt;IP-ADDRESSES&gt; - Specify the IP address(es) in the A.B.C.D format.</li> </ul> <p>This configuration triggers VRRP operation.</p>                                                                                                                                                                                                     |
| <b>preempt {delay &lt;1-65535&gt;}</b> | Controls whether a high priority backup router preempts a lower priority master. This field determines if a node with higher priority can takeover all virtual IPs from a node with lower priority. This feature is disabled by default. <ul style="list-style-type: none"> <li>• delay - Optional. Configures the pre-emption delay timer from 1 - 65535 seconds (default is 0 seconds). This option can be used to delay sending out the master advertisement or, in case of monitored link coming up, adjusting the VRRP priority by priority delta.</li> </ul> |
| <b>priority &lt;1-254&gt;</b>          | Configures the priority level of the router within a VRRP group. This value determines which node is elected as the Master. Higher values imply higher priority, value 254 has the highest precedence (default is 100).                                                                                                                                                                                                                                                                                                                                            |
| <b>sync-group</b>                      | Adds this VRRP group to a synchronized group. To trigger VRRP failover, it is essential all individual groups within a synchronized group have failover. VRRP failover is triggered if an advertisement is not received from the virtual masters that are part of this VRRP sync group. This feature is disabled by default.                                                                                                                                                                                                                                       |

```
vrrp <1-255> interface vlan <1-4094>
```

|                                      |                                                                                                                                                                                  |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vrrp &lt;1-255&gt;</b>            | Configures the virtual router ID from 1- 255. Identifies the virtual router the packet is reporting status for.                                                                  |
| <b>interface vlan &lt;1-4094&gt;</b> | Enables VRRP on the specified switch VLAN interface (SVI) <ul style="list-style-type: none"> <li>• vlan &lt;1-4094&gt; - Specify the VLAN interface ID from 1 - 4094.</li> </ul> |

```
vrrp <1-255> monitor critical-resource <CRM-NAME1> <CRM-NAME2> <CRM-NAME3> <CRM-NAME4>
(action [decrement-priority|increment-priority] {<IF-NAME>|pppoe1|vlan| wwan1})
```

|                                            |                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vrrp &lt;1-255&gt;</b>                  | Configures the virtual router ID from 1- 255. Identifies the virtual router the packet is reporting status for.                                                                                                                                                                                                            |
| <b>monitor</b>                             | Enables link monitoring or Critical Resource Monitoring (CRM)                                                                                                                                                                                                                                                              |
| <b>critical-resource &lt;CRM-NAME1&gt;</b> | Specifies the name of the critical resource to monitor. VRRP can be configured to monitor maximum of four critical resources. Use the <CRM-NAME2>, <CRM-NAME3>, and <CRM-NAME4> to provide names of the remaining three critical resources. By default VRRP is configured to monitor all critical resources on the device. |

|                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>action</b><br>[ <b>decrement-</b><br><b>priority</b>  <br><b>increment-</b><br><b>priority</b> ] | Sets the action on critical resource down event. It is a recursive parameter that sets the action for each of the four critical resources being monitored. <ul style="list-style-type: none"> <li>decrement-priority – Decrements the priority of virtual router on critical resource down event</li> <li>increment-priority – Increments the priority of virtual router on critical resource down event</li> </ul> |
| <b>&lt;IF-NAME&gt;</b>                                                                              | Optional. Enables interface monitoring <ul style="list-style-type: none"> <li>&lt;IF-NAME&gt; – Specify the interface name to monitor</li> </ul>                                                                                                                                                                                                                                                                    |
| <b>pppoe1</b>                                                                                       | Optional. Enables Point-to-Point Protocol (PPP) over Ethernet interface monitoring                                                                                                                                                                                                                                                                                                                                  |
| <b>vlan &lt;1-4094&gt;</b>                                                                          | Optional. Enables VLAN (switched virtual interface) interface monitoring <ul style="list-style-type: none"> <li>&lt;1-4094&gt; – Specify the VLAN interface ID from 1- 4094.</li> </ul>                                                                                                                                                                                                                             |
| <b>wwan1</b>                                                                                        | Optional. Enables Wireless WAN interface monitoring                                                                                                                                                                                                                                                                                                                                                                 |

```
vrrp <1-255> timers advertise [<1-255>|centiseconds <25-4095>|msec <250-999>]
```

|                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vrrp &lt;1-255&gt;</b>                                                                                                               | Configures the virtual router ID from 1- 255. Identifies the virtual router the packet is reporting status for.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>timers</b>                                                                                                                           | Configures the timer that runs every interval                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>advertise</b><br>[ <b>&lt;1-255&gt;</b>  <br><b>centiseconds</b><br><b>&lt;25-4095&gt;</b>   <b>msec</b><br><b>&lt;250-999&gt;</b> ] | Configures the VRRP advertisements time interval. This is the interval at which a master sends out advertisements on each of its configured VLANs. <ul style="list-style-type: none"> <li>&lt;1-255&gt; – Configures the timer interval from 1- 255 seconds. (applicable for VRRP version 2 only)</li> <li>centiseconds &lt;25-4095&gt; – Configures the timer interval in centiseconds (1/100th of a second). Specify a value between 25 - 4095 centiseconds (applicable for VRRP version 3 only).</li> <li>msec &lt;250-999&gt; – Configures the timer interval in milliseconds (1/1000th of a second). Specify a value between 250 - 999 msec (applicable for VRRP version 2 only).</li> </ul> <p>Default is 1 second.</p> |

```
vrrp version [2|3]
```

|                                     |                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vrrp version</b><br><b>[2 3]</b> | Configures one of the following VRRP versions: <ul style="list-style-type: none"> <li>2 – VRRP version 2 (RFC 3768). This is the default setting.</li> <li>3 – VRRP version 3 (RFC 5798 only IPV4)</li> </ul> <p>The VRRP version determines the router redundancy. Version 3 supports sub-second (centisecond) VRRP failover and support services over virtual IP.</p> |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Example

```
nx9500-6C8809(config-profile-default-rfs4000)#vrrp version 3
nx9500-6C8809(config-profile-default-rfs4000)#vrrp 1 sync-group
nx9500-6C8809(config-profile-default-rfs4000)#vrrp 1 delta-priority 100
nx9500-6C8809(config-profile-default-rfs4000)#show context
profile rfs4000 default-rfs4000
 bridge vlan 1

 vrrp 1 timers advertise 1
```

```
vrp 1 preempt
vrp 1 sync-group
vrp 1 delta-priority 100
vrp version 3
nx9500-6C8809(config-profile-default-rfs4000)#
```

### Related Commands

|                              |                       |
|------------------------------|-----------------------|
| <code>no</code> on page 1200 | Reverts VRRP settings |
|------------------------------|-----------------------|

### *vrp-state-check*

[Profile Config Commands](#) on page 862

Publishes interface via OSPF or BGP based on Virtual Router Redundancy Protocol (VRRP) status

VRRP allows automatic assignment of available IP routers to participating hosts. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP subnetwork. This option is enabled by default.

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
vrp-state-check
```

### Parameters

None

### Example

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#vrp-state-check

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context
nx9000 B4-C7-99-6C-88-09
 use profile default-nx9000
 use rf-domain default
.....
 no weight
 no timers bgp
 ip default-gateway priority 7500
 bgp-route-limit num-routes 10 retry-count 5 retry-timeout 60 reset-time 360
 vrp-state-check
 controller adopted-devices controllers
 alias string $SN B4C7996C8809
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```

### Related Commands

|                              |                                                                           |
|------------------------------|---------------------------------------------------------------------------|
| <code>no</code> on page 1200 | Disables the publishing of an interface via OSPF/BGP based on VRRP status |
|------------------------------|---------------------------------------------------------------------------|



## virtual-controller

[Profile Config Commands](#) on page 862

Enables an access point as a virtual-controller (VC) or a dynamic virtual controller (DVC)

When configured without the 'auto' option, this command manually enables an AP as a VC. The 'auto' option allows dynamic enabling of APs as VCs. When DVC is enabled on an AP's device or profile context, the AP is dynamically enabled as the VC on being elected as the RF-Domain manager.

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000



#### Note

The DVC feature is supported only on the AP7522, AP7532, AP7562, AP8432, and AP8533 model access points.

### Syntax

```
virtual-controller {auto|management-interface}
```

```
virtual-controller auto
```

```
virtual-controller {management-interface [ip address <IP/M>|vlan <1-4094>]}
```

### Parameters

```
virtual-controller auto
```

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>virtual-controller auto</b> | <p>Enables an AP as a virtual-controller</p> <ul style="list-style-type: none"><li>• auto – Enables AP as a DVC. When enabled, the AP on being elected as the RF Domain manager takes on the role of the virtual controller. In an RF-Domain, DVC can be enabled on multiple access points. However, only the current RF-Domain manager AP has a running instance of the DVC. This option is applicable only if enabling DVC.</li></ul> <p><b>Note:</b> MLCP discovery does not function on APs enabled as VC or DVCs. Do an explicit “mint link vlan X” on the AP's device/profile context, or “control-vlan X” in the AP's RF-Domain context, to establish MiNT links between the VC and its adopted APs.</p> |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
virtual-controller {management-interface [ip address <IP/M>|vlan <1-4094>]}
```

```

virtual-

controller

{management-

interface [ip

address <IP/M> |

vlan <1-4094>]}

```

**Note:** Enables an AP as a virtual-controller. If enabling DVC, use this option to configure management interface details.

- management-interface - Configures the management interface for the DVC. Configuring the management interface ensures failover in case the RF Domain manager is unreachable.
- ip address <IP/M> - Specify the management interface IP address. Due to the random nature of DVC, specifying an explicit management interface IP address makes it easier to manage VCs. In case of fail over, this IP address is installed as the secondary IP address on the new VC.
- vlan <1-4094> - Optional. Specifies the VLAN from 1 - 4094 on which the management interface IP address is configured.

For DVC, configuring management-interface ip address is mandatory. However, VLAN configuration is optional. If you configure the ip address without specifying the VLAN, the system configures the specified ip address as secondary ip on VLAN 1.

### Example

```

ap8533-9A1529(config-device-74-67-F7-9A-15-29)#virtual-controller auto

ap8533-9A1529(config-device-74-67-F7-9A-15-29)#virtual-controller management-interface ip
address 110.110.110.120/24

ap8533-9A1529(config-device-74-67-F7-9A-15-29)#virtual-controller management-interface
vlan 100

ap8533-9A1529(config-device-74-67-F7-9A-15-29)#show context | include virtual-controller
virtual-controller auto
virtual-controller management-interface ip address 110.110.110.120/24
virtual-controller management-interface vlan 100
ap8533-9A1529(config-device-74-67-F7-9A-15-29)#

```

The following example shows the management interface VLAN IP address being configured as the secondary IP address.

```

ap8533-9A1529(config-device-74-67-F7-9A-15-29)#show ip interface brief

INTERFACE IP-ADDRESS/MASK TYPE STATUS PROTOCOL

vlan1 10.1.1.11/24 primary UP up
vlan100 110.110.110.110/24 primary UP up
vlan100 110.110.110.120/24 secondary UP up

```

### wep-shared-key-auth

[Profile Config Commands](#) on page 862

Enables support for 802.11 WEP shared key authentication

When enabled, devices, using this profile, use a WEP key to access the network. The controller or service platform use the key algorithm to convert an ASCII string to the same hexadecimal number. Clients without the recommended adapters need to use WEP keys manually configured as hexadecimal numbers. This option is disabled by default.



### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

wep-shared-key-auth

### Parameters

None

### Example

```
nx9500-6C8809(config-profile-default-rfs4000)#wep-shared-key-auth

nx9500-6C8809(config-profile-default-rfs4000)#show context
profile rfs4000 default-rfs4000
 bridge vlan 1
 bridging-mode isolated-tunnel
 ip igmp snooping
 ip igmp snooping querier
 wep-shared-key-auth
 autoinstall configuration
 autoinstall firmware
 crypto ikev1 policy ikev1-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 interface mel
 interface gel
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
 interface ge2
 ip dhcp trust
--More--
nx9500-6C8809(config-profile-default-rfs4000)#
```

### Related Commands

|                                 |                                                           |
|---------------------------------|-----------------------------------------------------------|
| <a href="#">no</a> on page 1200 | Disables support for 802.11 WEP shared key authentication |
|---------------------------------|-----------------------------------------------------------|

*service*

[Profile Config Commands](#) on page 862

Service commands are used to view and manage configurations. The service commands and their corresponding parameters vary from mode to mode.

---

**Supported in the following platforms:**

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
service [captive-portal-server|cluster|critical-resource|fast-switching|
enable| global-association-list|lldp|memory|meshpoint|pm|power-config|
radius|remote-config|rss-timeout|watchdog|wireless|show]
```

```
service captive-portal-server connections-per-ip <3-64>
```

```
service cluster master-election immediate
```

```
service critical-resource port-mode-source-ip <IP>
```

```
service enable [l2tpv3|pppoe|radiusd]
```

```
service global-association-list blacklist-interval <1-65535>
```

```
service lldp loop-detection
```

```
service memory kernel decrease
```

```
service meshpoint loop-prevention-port [<L2-INTERFACE-NAME>|ge <1-5>|
port-channel <1-2>|up1]
```

```
service pm sys-restart
```

```
service power-config [3af-out|force-3at]
```

```
service radius dynamic-authorization additional-port <1-65535>
```

```
service remote-config apply-delay <0-600>
```

```
service rss-timeout <0-86400>
```

```
service watchdog
```

```
service wireless [anqp-frag-always|anqp-frag-size|ap650|client|cred-
cache-sync| inter-ap-key|noise-immunity|reconfig-on-tx-stall|test|wispe-
controller-port]
```

```
service wireless anqp-frag-always
```

```
service wireless anqp-frag-size <100-1500>
```

```
service wireless ap650 legacy-auto-update-image <FILE>
```

```
service wireless client tx-death on-radar-detect
```

```

service wireless cred-cache-sync [full|interval <30-864000>|never|
partial]
service wireless test [max-rate|max-retries|min-rate]
service wireless test [max-rate|min-rate]
[1,2,5.5,6,11,12,18,24,36,48,54,mcs0, mcs1,.....mcs23]
service wireless inter-ap-key [0 <WORD>|2 <WORD>|<WORD>]
service wireless noise-immunity
service wireless reconfig-on-rx-stall
service wireless test max-retries <0-15>
service wireless wispe-controller-port <1-65535>

service show cli

```

### Parameters

```
service captive-portal-server connections-per-ip <3-64>
```

|                                                              |                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>captive-portal-server connections-per-ip &lt;3-64&gt;</b> | <p>Configures the maximum number of simultaneous captive portal connection allowed per IP address</p> <ul style="list-style-type: none"> <li>• &lt;3-64&gt; - Specify the maximum number of connections per IP address from 3 - 64. The default is 3.</li> </ul> <p><b>Note:</b> This command is applicable only to the NX9XXX and NX9600 service platform profiles.</p> |
|--------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
service cluster master-election immediate
```

|                                          |                                                                                                                                                       |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>cluster master-election immediate</b> | <p>Initiates and completes cluster master election as soon as just one cluster member comes on and is active. This option is disabled by default.</p> |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|

```
service critical-resource port-mode-source-ip <IP>
```

|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>critical-resource port-mode-source-ip &lt;IP&gt;</b> | <p>Hard codes a source IP for critical resource management The default is 0.0.0.0 Use this option to define the IP address used as the source address in ARP packets used to detect a critical resource on a layer 2 interface. By default, the source address used in ARP packets to detect critical resources is 0.0.0.0. However, some devices do not support the above IP address and drop the ARP packets. Use this field to provide an IP address specifically used for this purpose. The IP address used for port-mode-source-ip monitoring must be different from the IP address configured on the device.</p> |
|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
service enable [l2tpv3|pppoe|radiusd]
```

|                               |                                                                                                                                                                           |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>service enable l2tpv3</b>  | Enables L2TPv3 on this profile<br>The L2TPV3 enable/disable option is not supported on AP6522, AP6562, AP7161, AP8163, AP8432, AP8533, RFS4000, and NX95XX model devices. |
| <b>service enable pppoe</b>   | Enables PPPoE features. When executed on a device, enables PPPoE on the logged device. When executed on a profile, enables PPPoE on all devices using that profile.       |
| <b>service enable radiusd</b> | Enables RADIUS features. When executed on a device, enables RADIUS on the logged device. When executed on a profile, enables RADIUS on all devices using that profile.    |

```
service global-association-list blacklist-interval <1-65535>
```

|                                           |                                                                                                                                                                                                                                                                               |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>service global-association-list</b>    | Configures global association list related parameters                                                                                                                                                                                                                         |
| <b>blacklist-interval &lt;1-65535&gt;</b> | Configures the period for which a client is blacklisted. A client is considered blacklisted after being denied access by the server. <ul style="list-style-type: none"> <li>• &lt;1-65535&gt; - Specify a value from 1 - 65535 seconds. The default is 60 seconds.</li> </ul> |

```
service lldp loop-detection
```

|                            |                                                                              |
|----------------------------|------------------------------------------------------------------------------|
| <b>lldp loop-detection</b> | Enables network loop detection via LLDP. This option is disabled by default. |
|----------------------------|------------------------------------------------------------------------------|

```
service memory kernel decrease
```

|                                       |                                                                                                                                                                                                                                |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>service memory kernel decrease</b> | Enables reduction in kernel memory usage. When enabled, firewall flows are reduced by 75% resulting in reduced kernel memory usage. A reboot is required for the option to take effect.<br>This option is disabled by default. |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
service meshpoint loop-prevention-port [<L2-INTERFACE-NAME>|ge <1-4>| port-channel <1-2>]
```

|                                       |                                                                                                                                                                                                            |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>meshpoint loop-prevention-port</b> | Limits meshpoint loop prevention to a single port                                                                                                                                                          |
| <b>&lt;L2-INTERFACE-NAME&gt;</b>      | Limits meshpoint loop prevention on a specified Ethernet interface <ul style="list-style-type: none"> <li>• &lt;L2-INTERFACE-NAME&gt; - Specify the layer 2 Ethernet interface name.</li> </ul>            |
| <b>ge &lt;1-4&gt;</b>                 | Limits meshpoint loop prevention on a specified GigabitEthernet interface <ul style="list-style-type: none"> <li>• ge &lt;1-4&gt; - Specify the GigabitEthernet interface index from 1 - 4.</li> </ul>     |
| <b>port-channel &lt;1-2&gt;</b>       | Limits meshpoint loop prevention on a specified port-channel interface <ul style="list-style-type: none"> <li>• port-channel &lt;1-2&gt; - Specify the port-channel interface index from 1 - 2.</li> </ul> |

```
service pm sys-restart
```

|                       |                                                                                                                 |
|-----------------------|-----------------------------------------------------------------------------------------------------------------|
| <b>pm sys-restart</b> | Enables the process monitor (PM) to restart the system when a process fails. This option is enabled by default. |
|-----------------------|-----------------------------------------------------------------------------------------------------------------|

```
service power-config [3af-out|force-3at]
```

|                               |                                                                                                       |
|-------------------------------|-------------------------------------------------------------------------------------------------------|
| <b>power-config 3af-out</b>   | Enables LLDP power negotiation, but uses 3af power. This option is disabled by default.               |
| <b>power-config force-3at</b> | Disables LLDP negotiation and forces 802.3at power configuration. This option is disabled by default. |

```
service radius dynamic-authorization additional-port <1-65535>
```

|                                                                     |                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>radius dynamic-authorization additional-port &lt;1-65535&gt;</b> | Configures an additional UDP port used by the device to listen for dynamic authorization messages <ul style="list-style-type: none"> <li>• &lt;1-65535&gt; - Specify a value from 1 - 65535. The default is 3799.</li> </ul> <p>The Cisco Identity Services Engine (ISE) server uses port 1700.</p> |
|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
service remote-config apply-delay <0-600>
```

|                                                |                                                                                                                                                                                                                                    |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>remote-config apply-delay &lt;0-600&gt;</b> | Delays configuration of a remote device (after it becomes active) by the specified time period <ul style="list-style-type: none"> <li>• &lt;0-600&gt; - Specify a value from 0 - 600 seconds. The default is 0 seconds.</li> </ul> |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
service rss-timeout <0-86400>
```

|                                    |                                                                                                                                                                                                                                                                                                     |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>rss-timeout &lt;0-86400&gt;</b> | Configures the duration, in seconds, for which an adopted access point will continue to provide wireless functions even after losing controller adoption. <ul style="list-style-type: none"> <li>• &lt;0-86400&gt; - Specify a value from 0 - 86400 seconds. The default is 300 seconds.</li> </ul> |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
service watchdog
```

|                 |                                                                                                                                                                                                                                            |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>watchdog</b> | Enables the watchdog. This feature is enabled by default. Enabling the watchdog option implements heartbeat messages to ensure other associated devices are up and running and capable of effectively inter-operating with the controller. |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
service wireless anqp-frag-always
```

|                                  |                                                                                |
|----------------------------------|--------------------------------------------------------------------------------|
| <b>wireless anqp-frag-always</b> | Enables fragmentation of all ANQP packets. This option is disabled by default. |
|----------------------------------|--------------------------------------------------------------------------------|

```
service wireless anqp-frag-size <100-1500>
```

|                                                 |                                                                                                                                                                       |
|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>wireless anqp-frag-size &lt;100-1500&gt;</b> | Configures the ANQP packet fragment size <ul style="list-style-type: none"> <li>• &lt;100-1500&gt; - Specify a value from 100 - 1500. The default is 1200.</li> </ul> |
|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
service wireless client tx-deauth on-radar-detection
```

|                                     |                                                                                                                                   |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <b>wireless client</b>              | Configures wireless client and stations related settings                                                                          |
| <b>tx-deauth on-radar-detection</b> | Enables access points to transmit deauth to clients when changing channels on radar detection. This option is enabled by default. |

```
service wireless cred-cache-sync [full|interval <30-864000>|never|partial]
```

|                                             |                                                                                                                                                                                                                             |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>wireless cred-cache-sync</b>             | Configures the credential cache's synchronization parameters. The parameters are: full, interval, never, and partial.                                                                                                       |
| <b>full</b>                                 | Enables synchronization of all credential cache entries                                                                                                                                                                     |
| <b>interval</b><br><b>&lt;30-864000&gt;</b> | Sets the interval, in seconds, at which the credential cache is synchronized <ul style="list-style-type: none"> <li>• &lt;30-864000&gt; - Specify a value from 30 - 864000 seconds. The default is 1200 seconds.</li> </ul> |
| <b>never</b>                                | Disables credential cache entry synchronization for all associated clients other than roaming clients. This is the default setting.                                                                                         |
| <b>partial</b>                              | Enables partial synchronization of parameters for associated clients, with credential cache close to aging out                                                                                                              |

```
service wireless inter-ap-key [0 <WORD> | 2 <WORD> | <WORD>]
```

|                                                         |                                                                                                   |
|---------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| <b>wireless inter-ap-key</b>                            | Configure encryption key used for securing inter-ap messages. This option is disabled by default. |
| <b>[ 0&lt;WORD&gt;   2&lt;WORD&gt;   &lt;WORD&gt; ]</b> | Specify a clear text or encrypted key.                                                            |

```
service wireless noise-immunity
```

|                                |                                                                                                      |
|--------------------------------|------------------------------------------------------------------------------------------------------|
| <b>wireless noise-immunity</b> | Polls for status and reconfigures radio in case of receive stall. This option is enabled by default. |
|--------------------------------|------------------------------------------------------------------------------------------------------|

```
service wireless reconfig-on-rx-stall
```

|                                      |                                     |
|--------------------------------------|-------------------------------------|
| <b>wireless reconfig-on-rx-stall</b> | Enables noise immunity on the radio |
|--------------------------------------|-------------------------------------|

```
service wireless test [max-rate|min-rate] [1,2,5.5,6,11,12,18,24,36,48,54,mcs0,mcs1,.....mcs23]
```

|                            |                                                                                                                                             |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <b>wireless test</b>       | Configures the serviceability parameters used for testing                                                                                   |
| <b>[max-rate min-rate]</b> | Configures the maximum and minimum data rates for clients using rate-scaling. The 'max-rate' and min-rate' options are disabled by default. |
| <b>[1,2,5.5,...mcs23]</b>  | Select the maximum and minimum data rates applicable.                                                                                       |

```
service wireless test max-retries <0-15>
```

|                                 |                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------|
| <b>wireless test</b>            | Configures the serviceability parameters used for testing                          |
| <b>max-retries &lt;0-15&gt;</b> | Configures the maximum number of retries per packet from 0 - 15. The default is 0. |

```
service wireless wispe-controller-port <1-65535>
```

|                                                        |                                                                                                                                                                                                                                                  |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>wispe-controller-port</b><br><b>&lt;1-65535&gt;</b> | Resets the Wireless Switch Protocol Enhanced (WISPe) controller port. This is the UDP port used to listen for WISPe. <ul style="list-style-type: none"> <li>• &lt;1-65535&gt; - Specify a value from 1 - 65535. The default is 24756.</li> </ul> |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

service show cli

|                 |                                                                                                                                                   |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>show cli</b> | Displays running system configuration details <ul style="list-style-type: none"> <li>• cli - Displays the CLI tree of the current mode</li> </ul> |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------|

### Example

```
nx9500-6C8809(config-profile-testRFS4000)#service radius dynamic-authorization additional-port 1700
```

```
nx9500-6C8809(config-profile-testRFS4000)#show context
profile rfs4000 testRFS4000
 service radius dynamic-authorization additional-port 1700
 no autoinstall configuration
 no autoinstall firmware
 crypto ikev1 policy ikev1-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
--More--
nx9500-6C8809(config-profile-testRFS4000)#
```

### Related Commands

|                        |                                              |
|------------------------|----------------------------------------------|
| <b>no</b> on page 1200 | Removes or resets service command parameters |
|------------------------|----------------------------------------------|

zone

[Profile Config Commands](#) on page 862

Configures the zone for devices using this profile. The zone can also be configured on the device's self context.

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
zone <NAME>
```

### Parameters

```
zone <NAME>
```

|                          |                                                                                                                                 |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>zone &lt;NAME&gt;</b> | Configures the device's zone/area <ul style="list-style-type: none"> <li>• &lt;NAME&gt; - Specify the zone/areaname.</li> </ul> |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------|

### Example

```
nx9500-6C8809(config-profile-testNX9000)#szone Ecospace

nx9500-6C8809(config-profile-testNX9000)#show context include-factory | include
zone
zone Ecospace
nx9500-6C8809(config-profile-testNX9000)#
```

### Related Commands

|                        |                                                       |
|------------------------|-------------------------------------------------------|
| <b>no</b> on page 1200 | Removes the zone configured on this profile or device |
|------------------------|-------------------------------------------------------|

## Device Config Commands

**PROFILES** on page 857

Use the (config) instance to configure device specific parameters

To navigate to this instance, use the following commands:

```
<DEVICE>(config)#<DEVICE-TYPE> <MAC>
<DEVICE>(config-device-<MAC>)#?
```

Device Mode commands:

|                                         |                                                                             |
|-----------------------------------------|-----------------------------------------------------------------------------|
| adopter-auto-provisioning-policy-lookup | Use centralized auto-provisioning policy when adopted by another controller |
| adoption                                | Adoption configuration                                                      |
| adoption-mode                           | Configure the adoption mode for the access-points in this RF-Domain         |
| adoption-site                           | Set system's adoption site                                                  |
| alias                                   | Alias                                                                       |
| application-policy                      | Application Policy configuration                                            |
| area                                    | Set name of area where the system is located?                               |
| arp                                     | Address Resolution Protocol (ARP)                                           |
| auto-learn                              | Auto learning                                                               |
| autogen-uniqueid                        | Autogenerate a unique id                                                    |
| autoinstall                             | Autoinstall settings                                                        |
| bridge                                  | Ethernet bridge                                                             |
| captive-portal                          | Captive portal                                                              |
| cdp                                     | Cisco Discovery Protocol                                                    |
| channel-list                            | Configure channel list to be advertised to wireless clients                 |
| cluster                                 | Cluster configuration                                                       |
| configuration-persistence               | Enable persistence of configuration across reloads (startup config file)    |
| contact                                 | Configure the contact                                                       |
| controller                              | WLAN controller configuration                                               |
| country-code                            | Configure the country of operation                                          |
| critical-resource                       | Critical Resource                                                           |
| crypto                                  | Encryption related commands                                                 |
| database                                | Database command                                                            |
| device-upgrade                          | Device firmware upgrade                                                     |
| device-onboard                          | Device-onboarding configuration                                             |
| dot1x                                   | 802.1X                                                                      |



|                                    |                                                                                 |
|------------------------------------|---------------------------------------------------------------------------------|
| dpi                                | Enable Deep-Packet-Inspection (Application Assurance)                           |
| dscp-mapping                       | Configure IP DSCP to 802.1p priority mapping for untagged                       |
| eguest-server                      | Enable EGuest Server functionality frames                                       |
| email-notification                 | Email notification configuration                                                |
| enforce-version                    | Check the firmware versions of devices before interoperating                    |
| environmental-sensor               | Environmental Sensors Configuration                                             |
| events                             | System event messages                                                           |
| export                             | Export a file                                                                   |
| file-sync                          | File sync between controller and adoptees                                       |
| floor                              | Set the floor within a area where the system is located                         |
| geo-coordinates                    | Configure geo coordinates for this device                                       |
| gre                                | GRE protocol                                                                    |
| hostname                           | Set system's network name                                                       |
| http-analyze                       | Specify HTTP-Analysis configuration                                             |
| interface                          | Select an interface to configure                                                |
| ip                                 | Internet Protocol (IP)                                                          |
| ipv6                               | Internet Protocol version 6 (IPv6)                                              |
| l2tpv3                             | L2tpv3 protocol                                                                 |
| l3e-lite-table                     | L3e lite Table                                                                  |
| lACP                               | LACP commands                                                                   |
| layout-coordinates                 | Configure layout coordinates for this device                                    |
| led                                | Turn LEDs on/off on the device                                                  |
| led-timeout                        | Configure the time for the led to turn off after the last radio state change    |
| legacy-auto-downgrade              | Enable device firmware to auto downgrade when other legacy devices are detected |
| legacy-auto-update                 | Auto upgrade of legacy devices                                                  |
| license                            | License management command                                                      |
| lldp                               | Link Layer Discovery Protocol                                                   |
| load-balancing                     | Configure load balancing parameter                                              |
| location                           | Configure the location                                                          |
| logging                            | Modify message logging facilities                                               |
| mac-address-table                  | MAC Address Table                                                               |
| mac-auth                           | 802.1X                                                                          |
| mac-name                           | Configure MAC address to name mappingss                                         |
| management-server                  | Configure management server address                                             |
| memory-profile                     | Memory profile to be used on the device                                         |
| meshpoint-device                   | Configure meshpoint device parameters                                           |
| meshpoint-monitor-interval         | Configure meshpoint monitoring interval                                         |
| min-misconfiguration-recovery-time | Check controller connectivity after configuration is received                   |
| mint                               | MinT protocol                                                                   |
| mirror                             | Mirroring                                                                       |
| misconfiguration-recovery-time     | Check controller connectivity after configuration is received                   |
| mpact-server                       | MPACT server configuration                                                      |
| neighbor-inactivity-timeout        | Configure neighbor inactivity timeout                                           |
| neighbor-info-interval             | Configure neighbor information exchange interval                                |

|                             |                                                                                     |
|-----------------------------|-------------------------------------------------------------------------------------|
| no                          | Negate a command or set its defaults                                                |
| noc                         | Configure the noc related setting                                                   |
| nsight                      | NSight                                                                              |
| nsight-sensor               | Enable sensor for Nsight                                                            |
| ntp                         | Ntp server A.B.C.D                                                                  |
| offline-duration            | Set duration for which a device remains unadopted before it generates offline event |
| otls                        | Omnitrail Location Server                                                           |
| override-wlan               | Configure RF Domain level overrides for wlan                                        |
| power-config                | Configure power mode                                                                |
| preferred-controller-group  | Controller group this system will prefer for adoption                               |
| preferred-tunnel-controller | Tunnel Controller Name this system will prefer for tunneling extended vlan traffic  |
| radius                      | Configure device-level radius authentication parameters                             |
| raid                        | RAID                                                                                |
| remove-override             | Remove configuration item override from the device (so profile value takes effect)  |
| rf-domain-manager           | RF Domain Manager                                                                   |
| router                      | Dynamic routing                                                                     |
| rsa-key                     | Assign a RSA key to a service                                                       |
| sensor-server               | AirDefense sensor server configuration                                              |
| slot                        | PCI expansion Slot                                                                  |
| spanning-tree               | Spanning tree                                                                       |
| timezone                    | Configure the timezone                                                              |
| traffic-class-mapping       | Configure IPv6 traffic class to 802.1p priority mapping for untagged frames         |
| traffic-shape               | Traffic shaping                                                                     |
| trustpoint                  | Assign a trustpoint to a service                                                    |
| tunnel-controller           | Tunnel Controller group this controller belongs to                                  |
| use                         | Set setting to use                                                                  |
| vrrp                        | VRRP configuration                                                                  |
| vrrp-state-check            | Publish interface via OSPF/BGP only if the interface VRRP state is not BACKUP       |
| wep-shared-key-auth         | Enable support for 802.11 WEP shared key authentication                             |
| zone                        | Configure Zone name                                                                 |
| clrscr                      | Clears the display screen                                                           |
| commit                      | Commit all changes made in this session                                             |
| do                          | Run commands from Exec mode                                                         |
| end                         | End current mode and change to EXEC mode                                            |
| exit                        | End current mode and down to previous mode                                          |
| help                        | Description of the interactive help system                                          |
| revert                      | Revert changes                                                                      |
| service                     | Service Commands                                                                    |
| show                        | Show running system information                                                     |
| write                       | Write running configuration to memory or terminal                                   |

<DEVICE>(config-device-<MAC>)#

The following table summarizes device configuration mode commands:

| Command                                                             | Description                                                                                                                                                                                                            |
|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">adopter-auto-provisioning-policy-lookup</a> on page 866 | Enables the use of a centralized auto provisioning policy on this device                                                                                                                                               |
| <a href="#">adoption</a> on page 867                                | Configures a minimum and maximum delay time in the initiation of the device adoption process                                                                                                                           |
| <a href="#">adoption-site</a> on page 1258                          | Sets the device's adoption site name                                                                                                                                                                                   |
| <a href="#">alias</a> on page 870                                   | Configures network, VLAN, and service aliases on a device                                                                                                                                                              |
| <a href="#">application-policy</a> on page 878                      | Associates a RADIUS server provided application policy with this device. When associated, the application policy allows wireless clients (MUs) to always find the RADIUS-supplied application policy in the dataplane. |
| <a href="#">area</a> on page 1259                                   | Sets the name of area where the system is deployed                                                                                                                                                                     |
| <a href="#">arp</a> on page 880                                     | Configures ARP parameters                                                                                                                                                                                              |
| <a href="#">auto-learn</a> on page 882                              | Enables controllers or service platforms to maintain a local configuration record of devices requesting adoption and provisioning. The command also enables learning of a device's host name via DHCP options.         |
| <a href="#">autogen-uniqueid</a> on page 883                        | When executed in the device configuration mode, this command generates a unique ID for the logged device                                                                                                               |
| <a href="#">autoinstall</a> on page 884                             | Autoinstalls firmware image and configuration setup parameters                                                                                                                                                         |
| <a href="#">bridge</a> on page 885                                  | Configures Ethernet Bridging parameters                                                                                                                                                                                |
| <a href="#">captive-portal</a> on page 913                          | Configures captive portal advanced Web page upload on this profile                                                                                                                                                     |
| <a href="#">cdp</a> on page 914                                     | Operates CDP on the device                                                                                                                                                                                             |
| <a href="#">channel-list</a> on page 1260                           | Configures channel list advertised to wireless clients                                                                                                                                                                 |
| <a href="#">cluster</a> on page 915                                 | Sets cluster configuration                                                                                                                                                                                             |
| <a href="#">configuration-persistence</a> on page 917               | Enables configuration persistence across reloads                                                                                                                                                                       |
| <a href="#">contact</a> on page 1261                                | Sets contact information                                                                                                                                                                                               |
| <a href="#">controller</a> on page 918                              | Configures a WLAN's wireless controller or service platform                                                                                                                                                            |
| <a href="#">country-code</a> on page 1261                           | Configures wireless controller or service platform's country code                                                                                                                                                      |
| <a href="#">critical-resource</a> on page 923                       | Monitors user configured IP addresses and logs their status                                                                                                                                                            |
| <a href="#">crypto</a> on page 931                                  | Configures data encryption protocols and settings                                                                                                                                                                      |
| <a href="#">database</a> on page 979                                | Backs up captive-portal and/or NSight database to a specified location and file and configures a low-disk-space threshold value                                                                                        |

| Command                                                 | Description                                                                                                                                                   |
|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">device-upgrade</a> on page 981              | Configures device firmware upgrade settings on this device                                                                                                    |
| <a href="#">diag</a> on page 983                        | Enables looped packet logging                                                                                                                                 |
| <a href="#">dot1x</a> on page 984                       | Configures 802.1x standard authentication controls                                                                                                            |
| <a href="#">dpi</a> on page 986                         | Enables Deep Packet Inspection (DPI) on this device                                                                                                           |
| <a href="#">dscp-mapping</a> on page 989                | Configures IP Differentiated Services Code Point (DSCP) to 802.1p priority mapping for untagged frames                                                        |
| <a href="#">eguest-server (VX9000 only)</a> on page 990 | Enables the EGuest daemon when executed without the 'host' option                                                                                             |
| <a href="#">eguest-server (NOC Only)</a> on page 991    | Points to the EGuest server, when executed along with the 'host' option                                                                                       |
| <a href="#">email-notification</a> on page 992          | Configures e-mail notification settings                                                                                                                       |
| <a href="#">enforce-version</a> on page 994             | Checks the device firmware version before attempting connection                                                                                               |
| <a href="#">environmental-sensor</a> on page 995        | Configures the environmental sensor device settings. If the device is an environmental sensor, use this command to configure its settings.                    |
| <a href="#">events</a> on page 998                      | Enables system event message generation and forwarding                                                                                                        |
| <a href="#">export</a> on page 998                      | Enables export of startup.log file after every boot                                                                                                           |
| <a href="#">file-sync</a> on page 999                   | Configures parameters enabling syncing of trustpoint/wireless-bridge certificate between the staging-controller and its adopted access points                 |
| <a href="#">floor</a> on page 1262                      | Sets the floor name where the system is located                                                                                                               |
| <a href="#">geo-coordinates</a> on page 1263            | Configures the geographic coordinates for this device                                                                                                         |
| <a href="#">gre</a> on page 1002                        | Enables GRE tunneling on this device                                                                                                                          |
| <a href="#">hostname</a> on page 1264                   | Sets a system's network name                                                                                                                                  |
| <a href="#">http-analyze</a> on page 1011               | Enables HTTP analysis on this device                                                                                                                          |
| <a href="#">interface</a> on page 1014                  | Selects an interface to configure                                                                                                                             |
| <a href="#">ip</a> on page 1154                         | Configures IPv4 components                                                                                                                                    |
| <a href="#">ipv6</a> on page 1162                       | Configures IPv6 components                                                                                                                                    |
| <a href="#">l2tpv3</a> on page 1167                     | Defines the Layer 2 Tunnel Protocol (L2TP) protocol for tunneling Layer 2 payloads using Virtual Private Networks (VPNs)                                      |
| <a href="#">l3e-lite-table</a> on page 1169             | Configures L3e Lite Table with this profile                                                                                                                   |
| <a href="#">lacp</a> on page 1265                       | Configures an LACP-enabled peer's system-priority value. LACP uses this system-priority value along with the peer's MAC address to form the peer's system ID. |
| <a href="#">layout-coordinates</a> on page 1266         | Configures layout coordinates                                                                                                                                 |
| <a href="#">led</a> on page 1169                        | Turns LEDs on or off                                                                                                                                          |

| Command                                                         | Description                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">led-timeout</a> on page 1170                        | Configures the LED-timeout timer in the device or profile configuration mode                                                                                                                                                                                                                      |
| <a href="#">legacy-auto-downgrade</a> on page 1171              | Enables legacy device firmware to auto downgrade                                                                                                                                                                                                                                                  |
| <a href="#">legacy-auto-update</a> on page 1172                 | Auto updates AP7161 legacy device firmware                                                                                                                                                                                                                                                        |
| <a href="#">license</a> on page 1267                            | Adds device feature licenses                                                                                                                                                                                                                                                                      |
| <a href="#">lldp</a> on page 1173                               | Configures Link Layer Discovery Protocol (LLDP) settings for this device                                                                                                                                                                                                                          |
| <a href="#">load-balancing</a> on page 1174                     | Configures load balancing parameters.                                                                                                                                                                                                                                                             |
| <a href="#">location</a> on page 1269                           | Configures the system's location (place of deployment)                                                                                                                                                                                                                                            |
| <a href="#">logging</a> on page 1180                            | Enables message logging                                                                                                                                                                                                                                                                           |
| <a href="#">mac-address-table</a> on page 1182                  | Configures the MAC address table                                                                                                                                                                                                                                                                  |
| <a href="#">mac-auth</a> on page 1183                           | Enables 802.1x authentication of hosts on this device                                                                                                                                                                                                                                             |
| <a href="#">mac-name</a> on page 1270                           | Configures MAC address to device name mappings                                                                                                                                                                                                                                                    |
| <a href="#">management-server</a> on page 1186                  | Configures a management server with this profile                                                                                                                                                                                                                                                  |
| <a href="#">meshpoint-device</a> on page 1187                   | Configures meshpoint device parameters                                                                                                                                                                                                                                                            |
| <a href="#">meshpoint-monitor-interval</a> on page 1188         | Configures meshpoint monitoring interval                                                                                                                                                                                                                                                          |
| <a href="#">min-misconfiguration-recovery-time</a> on page 1189 | Configures the minimum device connectivity verification time                                                                                                                                                                                                                                      |
| <a href="#">mint</a> on page 1190                               | Configures MiNT protocol settings                                                                                                                                                                                                                                                                 |
| <a href="#">misconfiguration-recovery-time</a> on page 1197     | Verifies device connectivity after a configuration is received                                                                                                                                                                                                                                    |
| <a href="#">neighbor-inactivity-timeout</a> on page 1198        | Configures neighbor inactivity timeout value                                                                                                                                                                                                                                                      |
| <a href="#">neighbor-info-interval</a> on page 1199             | Configures the neighbor information exchange interval                                                                                                                                                                                                                                             |
| <a href="#">no</a> on page 1271                                 | Negates a command or resets values to their default settings                                                                                                                                                                                                                                      |
| <a href="#">noc</a> on page 1202                                | Configures NOC settings                                                                                                                                                                                                                                                                           |
| <a href="#">nsight</a> on page 1272                             | Configures NSight database statistics related parameters. Use this command to set the interval at which data is updated by the RF Domain managers to the NSight server. This command is applicable only on the NX95XX series and NX9600 service platforms and is configured on the NSight server. |
| <a href="#">ntp</a> on page 1207                                | Configures NTP server settings                                                                                                                                                                                                                                                                    |
| <a href="#">offline-duration</a> on page 1212                   | Sets the duration, in minutes, for which a device remains unadopted before it generates offline event                                                                                                                                                                                             |

| Command                                                      | Description                                                                                                               |
|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <a href="#">override-wlan</a> on page 1276                   | Configures WLAN RF Domain level overrides on the logged device                                                            |
| <a href="#">power-config</a> on page 1213                    | Configures power mode features                                                                                            |
| <a href="#">preferred-controller-group</a> on page 1215      | Specifies the wireless controller or service platform group the system prefers for adoption                               |
| <a href="#">preferred-tunnel-controller</a> on page 1215     | Configures the tunnel wireless controller or service platform preferred by the system for tunneling extended VLAN traffic |
| <a href="#">radius</a> on page 1216                          | Configures device-level RADIUS authentication parameters                                                                  |
| <a href="#">remove-override</a> on page 1278                 | Removes device overrides                                                                                                  |
| <a href="#">rf-domain-manager</a> on page 1217               | Enables the RF Domain manager                                                                                             |
| <a href="#">router</a> on page 1218                          | Configures dynamic router protocol settings.                                                                              |
| <a href="#">rsa-key</a> on page 1280                         | Assigns a RSA key to SSH                                                                                                  |
| <a href="#">sensor-server</a> on page 1281                   | Configures an AirDefense sensor server                                                                                    |
| <a href="#">spanning-tree</a> on page 1220                   | Enables spanning tree commands on the logged device                                                                       |
| <a href="#">traffic-class-mapping</a> on page 1223           | Maps the IPv6 traffic class value of incoming IPv6 untagged packets to 802.1p priority                                    |
| <a href="#">traffic-shape</a> on page 1224                   | Enables traffic shaping and configures traffic shaping parameters on this device                                          |
| <a href="#">trustpoint (device-config-mode)</a> on page 1282 | Assigns trustpoints to validate various services, such as HTTPS, RADIUS CA, RADIUS server, external LDAP server, etc.     |
| <a href="#">timezone</a> on page 1282                        | Configures wireless controller or service platform's time zone settings                                                   |
| <a href="#">tunnel-controller</a> on page 1231               | Configures the tunneled WLAN (extended VLAN) wireless controller or service platform's name                               |
| <a href="#">use</a> on page 1232                             | Associates different policies and settings with this device                                                               |
| <a href="#">vrrp</a> on page 1238                            | Configures VRRP group settings                                                                                            |
| <a href="#">vrrp-state-check</a> on page 1242                | Publishes interface via OSPF or BGP based on Virtual Router Redundancy Protocol (VRRP) status                             |
| <a href="#">wep-shared-key-auth</a> on page 1244             | Enables support for 802.11 WEP shared key authentication                                                                  |
| <a href="#">raid</a> on page 1284                            | Enables alarm on the array. This command is supported only on the NX9500 series service platform.                         |

### *adoption-site*

[Device Config Commands](#) on page 1252

Sets the device's adoption site name

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
adoption-site <SITE-NAME>
```

### Parameters

```
adoption-site <SITE-NAME>
```

|                                                                                       |
|---------------------------------------------------------------------------------------|
| <b>adoption-site</b> Sets the device's adoption site name<br><b>&lt;SITE-NAME&gt;</b> |
|---------------------------------------------------------------------------------------|

### Example

```
rfs4000-229D58(config-device-00-23-68-22-9D-58)#adoption-site SanJoseMainOffice
```

### Related Commands

|                                                                           |
|---------------------------------------------------------------------------|
| <b>no</b> on page 1271      Disables or reverts settings to their default |
|---------------------------------------------------------------------------|

*area*

[Device Config Commands](#) on page 1252

Sets the physical area where the device (controller, service platform, or access point) is deployed. This can be a building, region, campus or other area that describes the deployment location of the device. Assigning an area name is helpful when grouping devices in RF Domains and profiles, as devices in the same physical deployment location may need to share specific configuration parameters in respect to radio transmission and interference requirements specific to that location.

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
area <AREA-NAME>
```

### Parameters

```
area <AREA-NAME>
```

|                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>area &lt;AREA-NAME&gt;</b> Sets the physical area where the device is deployed<br><b>&lt;AREA-NAME&gt;</b> <AREA-NAME> - Specify the area name (should not 64 characters in length). |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Example

```
nx9500-6C8809(config-device-00-04-96-4A-A7-08)#area RMZEcoSpace

nx9500-6C8809(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
 use profile default-ap71xx
 use rf-domain default
 hostname ap71361-4AA708
 area RMZEcospace
nx9500-6C8809(config-device-00-04-96-4A-A7-08)#
```

## Related Commands

|                              |                                               |
|------------------------------|-----------------------------------------------|
| <code>no</code> on page 1271 | Disables or reverts settings to their default |
|------------------------------|-----------------------------------------------|

### *channel-list*

[Device Config Commands](#) on page 1252

Configures the channel list advertised to wireless clients

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
channel-list [2.4GHz | 5GHz | dynamic]
channel-list [2.4GHz <CHANNEL-LIST> | 5GHz <CHANNEL-LIST> | dynamic]
```

### Parameters

```
channel-list [2.4GHz <CHANNEL-LIST> | 5GHz <CHANNEL-LIST> | dynamic]
```

|                                              |                                                                                                                                                                                                           |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>channel-list</b>                          | Configures the channel list advertised to wireless clients                                                                                                                                                |
| <b>2.4GHz</b><br><b>&lt;CHANNEL-LIST&gt;</b> | Configures the channel list advertised by radios operating in 2.4 GHz <ul style="list-style-type: none"><li>• &lt;CHANNEL-LIST&gt; - Specify a list of channels separated by commas or hyphens.</li></ul> |
| <b>5GHz &lt;CHANNEL-LIST&gt;</b>             | Configures the channel list advertised by radios operating in 5.0 GHz <ul style="list-style-type: none"><li>• &lt;CHANNEL-LIST&gt; - Specify a list of channels separated by commas or hyphens.</li></ul> |
| <b>dynamic</b>                               | Enables dynamic (neighboring access point based) update of configured channel list                                                                                                                        |

### Example

```
nx9500-6C8809(config-device-00-04-96-4A-A7-08)#channel-list 2.4GHz 1,2

nx9500-6C8809(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
 use profile default-ap71xx
 use rf-domain default
 hostname ap7161-4AA708
 area RMZEcospace
```



```
channel-list 2.4GHz 1,2
nx9500-6C8809(config-device-00-04-96-4A-A7-08)#
```

### Related Commands

|                                 |                                       |
|---------------------------------|---------------------------------------|
| <a href="#">no</a> on page 1271 | Resets the channel list configuration |
|---------------------------------|---------------------------------------|

### *contact*

[Device Config Commands](#) on page 1252

Defines an administrative contact for a deployed device (controller, service platform, or access point)

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
contact <WORD>
```

### Parameters

```
contact <WORD>
```

|                       |                                                                                     |
|-----------------------|-------------------------------------------------------------------------------------|
| <b>contact</b> <WORD> | Specify the administrative contact name (should not exceed 64 characters in length) |
|-----------------------|-------------------------------------------------------------------------------------|

### Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#contact Bob+1-631-738-5200
```

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
 use profile default-ap71xx
 use rf-domain default
 hostname ap7131-4AA708
 area RMZEospace
 contact Bob+1-631-738-5200
 channel-list 2.4GHz 1,2
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

### Related Commands

|                                 |                                        |
|---------------------------------|----------------------------------------|
| <a href="#">no</a> on page 1271 | Resets the administrative contact name |
|---------------------------------|----------------------------------------|

### *country-code*

[Device Config Commands](#) on page 1252

Defines the two digit country code for legal device deployment

Configuring the correct country is central to legal operation. Each country has its own regulatory restrictions concerning electromagnetic emissions and the maximum RF signal strength that can be transmitted.

**Supported in the following platforms:**

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

country-code <WORD>

**Parameters**

country-code <COUNTRY-CODE>

|                                                    |                                                                                                                                    |
|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| <b>country-code</b><br><b>&lt;COUNTRY-CODE&gt;</b> | Defines the two digit country code for legal device deployment<br>• <COUNTRY-CODE> - Specify the two letter ISO-3166 country code. |
|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|

**Example**

```
nx9500-6C8809(config-device-00-04-96-4A-A7-08)#country-code us

nx9500-6C8809(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
 use profile default-ap71xx
 use rf-domain default
 hostname ap7161-4AA708
 area RMZEcospace
 contact Bob+1-631-738-5200
 country-code us
 channel-list 2.4GHz 1,2
nx9500-6C8809(config-device-00-04-96-4A-A7-08)#
```

**Related Commands**

|                                 |                                     |
|---------------------------------|-------------------------------------|
| <a href="#">no</a> on page 1271 | Removes the configured country code |
|---------------------------------|-------------------------------------|

*floor*

[Device Config Commands](#) on page 1252

Sets the building floor name representative of the location within the area or building the device (controller, service platform, or access point) is physically deployed. Assigning a building floor name is helpful when grouping devices in RF Domains and profiles, as devices on the same physical building floor may need to share specific configuration parameters in respect to radio transmission and interference requirements specific to that location.

**Supported in the following platforms:**

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533



- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
floor <FLOOR-NAME> <1-4094>
```

### Parameters

```
floor <FLOOR-NAME> <1-4094>
```

|                                                       |                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>floor &lt;FLOOR-NAME&gt; &lt;1-4094&gt;</b></p> | <p>Sets the building floor name where the device is deployed</p> <ul style="list-style-type: none"> <li>• &lt;1-4094&gt; - Sets a numerical floor designation in respect to the floor's actual location within a building. Specify a value from 1 - 4094. The default setting is the 1st floor.</li> </ul> |
|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Example

```
nx9500-6C8809(config-device-00-04-96-4A-A7-08)#floor 5thfloor
```

```
nx9500-6C8809(config-device-00-04-96-4A-A7-08)#show context
```

```
ap71xx 00-04-96-4A-A7-08
 use profile default-ap71xx
 use rf-domain default
 hostname ap7161-4AA708
 area RMZEcospace
 floor 5thfloor
 contact Bob+1-631-738-5200
 country-code us
 channel-list 2.4GHz 1,2
nx9500-6C8809(config-device-00-04-96-4A-A7-08)#
```

### Related Commands

|                               |                                             |
|-------------------------------|---------------------------------------------|
| <p><b>no</b> on page 1271</p> | <p>Removes device's location floor name</p> |
|-------------------------------|---------------------------------------------|

### *geo-coordinates*

[Device Config Commands](#) on page 1252

Configures the geographic coordinates for this device. Specifies the exact location of this device in terms of latitude and longitude coordinates.

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
geographic coordinates <-90.0000-90.0000> <-180.0000-180.0000>
```

## Parameters

geographic coordinates <-90.0000-90.0000> <-180.0000-180.0000>

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>geographic coordinates</b> | <p>Configures the geographic coordinates for this device</p> <ul style="list-style-type: none"><li>• &lt;-90.0000-90.0000&gt; - Specify the device's latitude coordinate from -90.0000 to 90.0000. When looking at a floor map, latitude lines specify the east-west position of a point on the Earth's surface.</li><li>• &lt;-180.0000-180.0000&gt; - Specify the device's longitude coordinate from -180.0000 to 180.0000. When looking at a floor map, longitude lines specify the north-south position of a point on the Earth's surface.</li></ul> |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Example

```
rfs4000-229D58(config-device-00-23-68-22-9D-58)#geo-coordinates -90.0000 166.0000

rfs4000-229D58(config-device-00-23-68-22-9D-58)#show context
rfs4000 00-23-68-22-9D-58
 use profile default-rfs4000
 use rf-domain default
 hostname rfs4000-229D58
 geo-coordinates -90.0000 166.0000
 license AP DEFAULT-6AP-LICENSE
 license ADSEC DEFAULT-ADV-SEC-LICENSE
 ip default-gateway 192.168.13.2
 ip default-gateway priority static-route 20
 interface gel
 switchport mode access
 switchport access vlan 1
 interface vlan1
 ip address 192.168.13.9/24
 ip address 192.168.0.1/24 secondary
 ip dhcp client request options all
 use client-identity-group ClientIdentityGroup
 logging on
 logging console warnings
 logging buffered warnings
rfs4000-229D58(config-device-00-23-68-22-9D-58)#
```

## Related Commands

|                        |                                         |
|------------------------|-----------------------------------------|
| <b>no</b> on page 1271 | Removes device's geographic coordinates |
|------------------------|-----------------------------------------|

*hostname*

[Device Config Commands](#) on page 1252

Sets the system's network name

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

## Syntax

hostname <WORD>

## Parameters

hostname <WORD>

|                                                                                                                                                                           |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>hostname &lt;WORD&gt;</b> Sets the name of the managing wireless controller, service platform, or access point. This name is displayed when accessed from any network. |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Example

```
nx9500-6C8809(config-device-00-04-96-4A-A7-08)#hostname TechPubAP7161
```

The hostname has changed from 'ap7131-4AA708' to 'TechPubAP7161'

```
nx9500-6C8809(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
 use profile default-ap71xx
 use rf-domain default
 hostname TechPubAP7161
 area RMZEcospace
 floor 5thfloor
 contact Bob+1-631-738-5200
 country-code us
 channel-list 2.4GHz 1,2
nx9500-6C8809(config-device-00-04-96-4A-A7-08)#
```

## Related Commands

|                        |                           |
|------------------------|---------------------------|
| <b>no</b> on page 1271 | Removes device's hostname |
|------------------------|---------------------------|

*lACP*

[Device Config Commands](#) on page 1252

Configures an LACP-enabled peer's system priority value. LACP uses this system priority value along with the peer's MAC address to form the system ID. In a LAG, the peer with the lower system ID initiates LACP negotiations with another peer. In scenarios, where both peers have the same system-priority value assigned, the peer with the lower MAC gets precedence.



### Note

For more information on enabling link aggregation, see [lACP](#) on page 1029 and [lACP-channel-group](#) on page 1029.

## Supported in the following platforms:

- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

## Syntax

lACP system-priority <1-65535>

## Parameters

lACP system-priority <1-65535>

**lACP system-priority**  
**<1-65535>**

Configures the LACP system priority value

- <1-65535> - Specify a value from 1 - 65535. Lower the value, higher is the priority. Therefore, '1' and '65535' indicate highest and lowest system-priority values respectively. The default value is 32768.

### Example

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#lACP system-priority 1
```

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context include-factory | include lACP
lACP system-priority 1
lACP channel-group 1 mode active
lACP port-priority 2
lACP channel-group 1 mode active
lACP port-priority 2
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```

### Related Commands

**no** on page 1271

Removes this device's configured system-priority value

*layout-coordinates*

[Device Config Commands](#) on page 1252

Configures X and Y layout coordinates for the device

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
layout-coordinates <-4096.0-4096.0> <-4096.0-4096.0>
```

### Parameters

```
layout-coordinates <-4096.0-4096.0> <-4096.0-4096.0>
```

**layout-coordinates**

Configures X and Y layout coordinates for the device

**<-4096.0-4096.0>** Specify the X coordinate from -4096 - 4096.0  
>

**<-4096.0-4096.0>** Specify the Y coordinate from -4096 - 4096.0  
>

### Example

```
nx9500-6C8809(config-device-00-04-96-4A-A7-08)#layout-coordinates 1.0 2.0
```

```
nx9500-6C8809(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
```

```
use profile default-ap71xx
use rf-domain default
hostname TechPubAP7161
area RMZEcospace
floor 5thfloor
layout-coordinates 1.0 2.0
contact Bob+1-631-738-5200
country-code us
channel-list 2.4GHz 1,2
nx9500-6C8809(config-device-00-04-96-4A-A7-08)#
```

## Related Commands

|                              |                                      |
|------------------------------|--------------------------------------|
| <code>no</code> on page 1271 | Removes device's layout co-ordinates |
|------------------------------|--------------------------------------|

### *license*

[Device Config Commands](#) on page 1252

Adds a license pack on the device for the specified feature (AP/AAP/ADSEC/HTANLT/WEBF/NSIGHT/NSIGHT-PER/EGUEST-DEV)

The WiNG HM network defines a three-tier structure, consisting of multiple wireless sites managed by a single Network Operations Center (NOC) controller, The NOC controller constitutes the first and the site controllers constitute the second tier of the hierarchy. The site controllers may or may not be grouped to form clusters. The site controllers in turn adopt and manage access points that form the third tier of the hierarchy.

The NOC controllers and/or site controllers can both have license packs installed. Adoption of APs by the NOC and site controllers depends on the number of licenses available on each of these controllers.

The NOC controllers and/or site controllers can both have license packs installed. When a AP is adopted by a site controller, the site controller pushes a license on to the AP. The various possible scenarios are:

- AP licenses installed only on NOC controller:

The NOC controller provides the site controllers with AP licenses, ensuring that per platform limits are not exceeded.

- AP licenses installed on site controller:

The site controller uses its installed licenses, and then asks the NOC controller for additional licenses in case of a shortage.

In a hierarchical and centrally managed network, the NOC controller can pull unused AP licenses from site controllers and relocate to other site controllers when required.

- AP licenses installed on any member of a site cluster:

The site controller shares installed and borrowed (from the NOC) licenses with other controllers within a site cluster.

### **Supported in the following platforms:**

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000

- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

license <WORD> <LICENSE-KEY>

### Parameters

license <WORD> <LICENSE-KEY>

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;WORD&gt;</b>        | <p>Specify the feature name (AP/AAP/ADSEC/HTANLT/WEBF/NSIGHT/NSIGHT-PER/EGUEST-DEV) for which license is added.</p> <ul style="list-style-type: none"> <li>• AP License: This is the license key required for AP adoptions. The number of APs that can be adopted depends on the installed license count. If the installed license count is 10 APs and the number of AP adoptions is 5, 5 additional APs can still be adopted under the terms of the license.</li> <li>• AAP License: This is the license key required for AAP adoptions. The number of AAPs that can be adopted depends on the installed license count. If the installed license count is 10 APs and the number of AAP adoptions is 5, 5 additional AAPs can still be adopted under the terms of the license.</li> <li>• ADSEC License: This is the license key required to install the Role Based Firewall feature and increase the number of IPSec VPN tunnels. The number of IPSec tunnels varies by platform.</li> <li>• HTANLT: This is the license key required to install Analytics (an enhanced statistical management tool) for NX95XX series service platforms.</li> <li>• WEBF License: This is the license key required to install the Web filtering feature. Web filtering is used to restrict access to specific resources on the Internet.</li> <li>• NSIGHT/NSIGHT-PER Licenses: This is the license key required to install NSight on a supported service platform. The NSight UI displays a comprehensive, day-to-day overview of the network in a graphical, visually interactive, and easy-to-use format. However, NSight being a licensed service, on expiration of the first 120 days grace period, the NSight server's NSight UI can be launched only on the application of the NSight or NSight-Per (NSight Perpetual) license.</li> </ul> <p>The difference between the NSight and NSight-Per licenses is that the first one has an expiration date, whereas the latter doesn't have an expiration date. Once purchased and applied, the NSight-Per license is active forever, and is therefore ideally suited for a Replica-set, NSight deployment, where it is essential that the license is perpetually active and synched across the NSight servers and their primary and secondary databases.</p> <p><b>Note:</b> NSight is supported only on NX9500, NX9510, NX9600 model service platforms, and the VX9000 virtual controller.</p> <ul style="list-style-type: none"> <li>• EGUEST-DEV License - This is the per-device license key installed on the EGuest server. Once installed the EGuest feature is activated. The EGuest-DEV license defines the number of APs supported by each EGuest server. The maximum limit for per-device license is 100,000.</li> </ul> <p>The EGuest server is supported only on the VX9000 platform.</p> |
| <b>&lt;LICENSE-KEY&gt;</b> | Specify the license key.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

### Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#license ap aplicensekey@1234
aplicensekey@123
```



```

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
 use profile default-ap71xx
 use rf-domain default
 hostname TechPubAP7131
 floor 5thfloor
 layout-coordinates 1.0 2.0
 license AP aplicensekey@1234 aplicensekey@123
 location SanJose
 no contact
 country-code us
 channel-list 2.4GHz 1,2
 mac-name 00-04-96-4A-A7-08 5.8TestAP
 neighbor-info-interval 50
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#license NSIGHT 62e512ae6cb74689df
253a03efe493f375597b67c70ee0b7c30655256b1322d064ca8dfaecedc450

VX-EGuest-DB(config-device-14-A0-19-06-AB-10)#license EGUEST-DEV
5f06f09e8209cba1fc7db70681fe78ba2707bbcd6ca2e8f8a31fe5b7e2e778c8b0d0ee3994f800ad
VX-EGuest-DB(config-device-14-A0-19-06-AB-10)#commit write

VX-EGuest-DB(config-device-14-A0-19-06-AB-10)#show context include-factory | include
license
 license EGUEST-DEV
5f06f09e8209cba1fc7db70681fe78ba2707bbcd6ca2e8f8a31fe5b7e2e778c8b0d0ee3994f800ad
VX-EGuest-DB(config-device-14-A0-19-06-AB-10)#

```

## location

[Device Config Commands](#) on page 1252

Sets the location where a managed device (controller, service platform, or access point) is deployed. This is the location of the device with respect to the RF Domain it belongs.

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
location <WORD>
```

### Parameters

```
location <WORD>
```

**<WORD>**

Specify the managed device's location as part of its RF Domain configuration

### Example

```

nx9500-6C8809(config-device-00-04-96-4A-A7-08)#location SanJose

nx9500-6C8809(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08

```

```

use profile default-ap7lxx
use rf-domain default
hostname TechPubAP7161
area RMZEcospace
floor 5thfloor
layout-coordinates 1.0 2.0
location SanJose
contact Bob+1-631-738-5200
country-code us
channel-list 2.4GHz 1,2
nx9500-6C8809(config-device-00-04-96-4A-A7-08)#

```

## Related Commands

|                                 |                                     |
|---------------------------------|-------------------------------------|
| <a href="#">no</a> on page 1271 | Removes a managed device's location |
|---------------------------------|-------------------------------------|

### *mac-name*

[Device Config Commands](#) on page 1252

Configures a client name to MAC address mapping. Use this command to assign a user-friendly name to the device (controller, service platform, or access point) and map it to the device's MAC address.

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
mac-name <MAC> <NAME>
```

### Parameters

```
mac-name <MAC> <NAME>
```

|                             |                                                                                                                                                                                                                                                    |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mac-name &lt;MAC&gt;</b> | Maps a user-friendly name to the device's MAC address                                                                                                                                                                                              |
| <b>&lt;NAME&gt;</b>         | <ul style="list-style-type: none"> <li>• &lt;MAC&gt; – Specify the device's MAC address.</li> <li>• &lt;NAME&gt; – Specify the 'friendly' name used for the specified MAC address. This is the name used in events and statistics logs.</li> </ul> |

### Example

```
nx9500-6C8809(config-device-00-04-96-4A-A7-08)#mac-name 00-04-96-4A-A7-08 5.8TestAP
```

```

nx9500-6C8809(config-device-00-04-96-4A-A7-08)#show context
ap7lxx 00-04-96-4A-A7-08
use profile default-ap7lxx
use rf-domain default
hostname TechPubAP7161
area RMZEcospace
floor 5thfloor
layout-coordinates 1.0 2.0
location SanJose
contact Bob+1-631-738-5200

```

```
country-code us
channel-list 2.4GHz 1,2
mac-name 00-04-96-4A-A7-08 5.8TestAP
nx9500-6C8809(config-device-00-04-96-4A-A7-08)#
```

## Related Commands

|                                 |                                                           |
|---------------------------------|-----------------------------------------------------------|
| <a href="#">no</a> on page 1271 | Removes the device's friendly name to MAC address mapping |
|---------------------------------|-----------------------------------------------------------|

*no*

[Device Config Commands](#) on page 1252

Negates a command or resets values to their default

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
no [adopter-auto-provisioning-policy-lookup|adoption-site|alias|
application-policy|area|arp|auto-learn-staging-config|autoinstall|bridge|
captive-portal| cdp|channel-list|cluster|configuration-persistence|
contact|controller| country-code|critical-resource|crypto|database-
backup|device-upgrade|dot1x| dpi|dscp-mapping|email-notification|
environmental-sensor|events|export| file-sync|floor|geo-coordinates|gre|
hostname|http-analyze|interface|ip|ipv6| l2tpv3|l3-lite-table|lacp|
layout-coordinates|led|led-timeout| legacy-auto-downgrade|legacy-auto-
update|license|lldp|load-balancing|location| logging|mac-address-table|
mac-auth|mac-name|management-server|memory-profile| meshpoint-device|
meshpoint-monitor-interval|min-misconfiguration-recovery-time| mint|
mirror|misconfiguration-recovery-time|mpact-server|noc|nsight| |ntp|
offline-duration|override-wlan|power-config|preferred-controller-group|
preferred-tunnel-controller|radius|raid|rf-domain-manager|router|rsa-key|
sensor-server|slot|spanning-tree|timezone|traffic-class-mapping|traffic-
shape| trustpoint|tunnel-controller|use|vrrp|vrrp-state-check|wep-shared-
key-auth| service]
```

### Parameters

```
no <PARAMETERS>
```

|                        |                                                                               |
|------------------------|-------------------------------------------------------------------------------|
| <b>no</b> <PARAMETERS> | Removes or resets the logged device's settings based on the parameters passed |
|------------------------|-------------------------------------------------------------------------------|

### Usage Guidelines

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated

## Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#no area
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#no contact
```

*nsight*

[Device Config Commands](#) on page 1252

Configures NSight database related parameters. Use this command to configure the data-update periodicity, number of applications posted to the NSight server for a wireless client, and the duration for which data is stored in the NSight database's buckets. These parameters impact the amount of data stored in the NSight DB and interval at which data is aggregated and expired within the NSight DB. For more information on data aggregation and expiration, see [Usage Guidelines \(Data Aggregation and Expiration\)](#) on page 1274.

Configure these parameters in the NSight server's device configuration mode.

### Supported in the following platforms:

- Service Platforms — NX9500, NX9510, NX9600, VX9000

### Syntax

```
nsight database [statistics|summary]
```

```
nsight database statistics [avc-update-interval|max-apps-per-client|
update-interval|wireless-clients-update-interval]
```

```
nsight database statistics [avc-update-interval|update-interval|wireless-
clients-update-interval] [120|30|300|60|600]
```

```
nsight database statistics max-apps-per-client <1-1000>
```

```
nsight database summary duration <1-24> <1-168> <1-2160> <24-26280>
```

### Parameters

```
nsight database statistics [avc-update-interval|update-interval|wireless-clients-update-
interval] [120|30|300|60|600]
```

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>nsight database</b>     | Configures NSight database statistics related parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>statistics</b>          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>avc-update-interval</b> | Configures the interval, in seconds, at which Application Visibility and Control (AVC) statistics is updated to the NSight database. This interval represents the rate at which AVC-related data is inserted in the NSight database's first bucket. This first bucket data is referred to as the RAW records. A bucket is a database collection that holds statistical data on a per RF Domain basis. For more information, see <a href="#">Usage Guidelines (Data Aggregation and Expiration)</a> on page 1274.<br>When configured, RF Domain managers posting AVC-related data to the NSight server receive a reply from the NSight server intimating the next update time. The NSight server calculates the 'next update time' based on the avc-update-interval configured here. |

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>update-interval</b>                  | <p>Configures the interval, in seconds, at which data is updated to the NSight server. This interval represents the rate at which data (excluding AVC and wireless-clients related statistics) is inserted in the NSight database's first bucket. This first bucket data is referred to as the RAW records. A bucket is a database collection that holds statistical data on a per RF Domain basis. For more information, see <a href="#">Usage Guidelines (Data Aggregation and Expiration)</a> on page 1274.</p> <p>When configured, RF Domain managers posting data to the NSight server receive a reply from the NSight server intimating the next update time. The NSight server calculates the 'next update time' based on the update-interval configured here.</p> <p><b>Note:</b> Use the 'avc-update-interval' and 'wireless-clients-update-interval' keywords to configure update interval for AVC-related and wireless-clients related information respectively.</p> |
| <b>wireless-clients-update-interval</b> | <p>Configures the interval, in seconds, at which wireless-client statistics is updated to the NSight server. This interval represents the rate at which wireless-clients related statistics is inserted in the NSight database's first bucket. This first bucket data is referred to as the RAW records. A bucket is a database collection that holds statistical data on a per RF Domain basis. For more information, see <a href="#">Usage Guidelines (Data Aggregation and Expiration)</a> on page 1274.</p> <p>When configured, RF Domain managers posting wireless-client related data to the NSight server receive a reply from the NSight server intimating the next update time. The NSight server calculates the 'next update time' based on the wireless-clients-update-interval configured here.</p>                                                                                                                                                                 |
| <b>[120   30   300   60   600]</b>      | <p>The following keywords are common to all of the above parameters:</p> <ul style="list-style-type: none"> <li>• 120 – Sets the data-update periodicity as 120 seconds (2 minutes)</li> <li>• 30 – Sets the data-update periodicity as 30 seconds</li> <li>• 300 – Sets the data-update periodicity as 300 seconds (5 minutes). This is the default setting for the 'avc-update-interval' and 'wireless-clients-update-interval' parameters.</li> <li>• 60 – Sets the data-update periodicity as 60 seconds (1 minute). This is the default setting for the 'update-interval' parameter.</li> <li>• 600 – Sets the data-update periodicity as 600 seconds (10 minutes)</li> </ul>                                                                                                                                                                                                                                                                                              |

```
nsight database statistics max-apps-per-client <1-1000>
```

|                                   |                                                                                                                                                                                                                                                       |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>nsight database statistics</b> | Configures NSight database statistics related parameters                                                                                                                                                                                              |
| <b>max-apps-per-client</b>        | Configures the maximum number of applications per wireless-client to be posted to the NSight server within the configured data-update interval. This information is included in the AVC statistics posted by RF Domain managers to the NSight server. |
| <b>&lt;1-1000&gt;</b>             | Specify the number of applications posted from 1 - 1000. The default is 10 applications per wireless client.                                                                                                                                          |

```
nsight database summary duration <1-24> <1-168> <1-2160> <24-26280>
```



|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>nsight database summary</b> | Configures the NSight database's per-bucket data storage duration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>duration &lt;1-24&gt;</b>   | Configures the duration for which data is stored on a per-bucket basis                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>&lt;1-168&gt;</b>           | <ul style="list-style-type: none"> <li>• &lt;1-24&gt; – Specify the bucket 1 duration from 1 - 24 hours (i.e. 1 hour to 1 day). The default is 8 hours.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>&lt;1-2160&gt;</b>          | <ul style="list-style-type: none"> <li>• &lt;1-168&gt; – Specify the bucket 2 duration from 1 - 168 hours (i.e. 1 hour to 7 days). The default is 24 hours.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>&lt;24-26280&gt;</b>        | <ul style="list-style-type: none"> <li>• &lt;1-2160&gt; – Specify the bucket 3 duration from 1 - 2160 hours (i.e. 1 hour to 90 days). The default is 7 days (168 hours).</li> <li>• &lt;24-26280&gt; – Specify the bucket 4 duration from 24 - 26280 hours (i.e. 1 day to 3 years). The default is 365 days (1 year).</li> </ul> <p><b>Note:</b> A bucket is a database collection that holds statistical data for each RF Domain within the network. (Note, only those RF Domain's that are using an NSight policy with the NSight server host configured will post data to the NSight server. For more information, see <a href="#">use (rf-domain-config-mode)</a> on page 524 in the RF Domain configuration mode.) NSight database has four (4) buckets. The data from each bucket is aggregated and pushed to the next bucket once the data storage duration, specified for the bucket, has exceeded. For more information on data aggregation, see <a href="#">Usage Guidelines (Data Aggregation and Expiration)</a>.</p> |

### Usage Guidelines (Data Aggregation and Expiration)

Data Aggregation:

The NSight functionality, a data analytics tool, analyzes data that is generated periodically by the nodes within the managed wireless LAN. For large WLAN networks, generating significantly large amount of data, storing data forever is neither feasible nor beneficial. Therefore, older statistics are summarized into aggregated (averaged) records. All records, for a fixed time period in past, are summarized into one record by taking an average of them. Although this causes a loss in the data's granularity, average numbers for any given time period is still available.

Statistical data periodically posted by RF Domain managers to the NSight server are stored in buckets (database collections) within the NSight database. There are four buckets in total. These are:

- First bucket (termed as the RAW bucket) - B1
- Second bucket - B2
- Third bucket - B3
- Fourth bucket - B4

On completion of the data storage duration, records from a bucket are aggregated (at a fixed rate) and inserted into the next bucket. The rate at which records are aggregated into the next bucket becomes the next bucket's granularity. For example, the B1 records (that have exceeded the data storage duration configured for B1) are aggregated (at the rate specified) and inserted into B2. Similarly, data from B2 are aggregated into B3, and from B3 to B4. The fixed rate of aggregation (or granularity) AND default storage duration for each bucket is as follows:

- B1: storage duration 8 hours
- B2: granularity 10 minutes / storage duration 24 hours
- B3: granularity 1 hour / storage duration 7 days
- B4: granularity 1 day / storage duration 1 year

Let us consider (with default update-interval settings) the growth of any one of the statistical buckets.

- Since B1's default data storage duration is 8 hours, B1 will hold a maximum of 960 records per RF Domain after 8 hours (updated at the rate of 30 seconds).
- Since B2's granularity is 10 minutes, every 10 minutes 20 records from the B1 will be aggregated into a single record and inserted into B2.
- Since B2's default storage duration is 24 hours, it will contain a maximum of 144 records per RF Domain after 24 hours.
- Since B3's granularity is 1 hour, every hour 6 records from B2 will be aggregated into a single record and inserted into B3.
- Since B3's default storage duration is 7 days, it will contain a maximum of 168 records per RF Domain after 7 days.
- Since B4's granularity is 1 day, every day 24 records from B3 will be aggregated into a single record and inserted into B4.
- Since B4's default storage duration is 365 days, it will contain a maximum of 365 records per RF Domain after 1 year.

Data Expiration:

The expiration of older records (also referred to as purging or deleting of records) occurs along with data aggregation for each bucket.

Let us consider (with default data storage-duration settings) the expiration of data for any one of the statistical buckets.

- As stated earlier, at the end of 8 hours B1 will have 960 records per RF Domain. After a period of 8 hours and 10 minutes, all 960 records are aggregated into 144 records and inserted into B2. To enable B1 to hold exactly 8 hours worth of data, 20 of the oldest records (corresponding to the first 10 minutes) are purged from B1 at the end of 8 hours and 10 minutes. This expiration cycle is triggered every 10 minutes.
- At the end of 24 hours B2 will have 144 records per RF Domain. After a period of 24 hours and 10 minutes, one of the oldest record (corresponding to the first 10 minutes) is purged from B2. This expiration cycle is triggered every 10 minutes to enable B2 to maintain exactly 24 hours worth of data.
- At the end of 7 days B3 will have 168 records per RF Domain. After a period of 7 days and one hour one of the oldest record (corresponding to the first hour) is purged from B3. This expiration cycle is triggered every 1 hour to enable B3 to maintain exactly 7 days worth of data.
- At the end of 365 days B4 will have 365 records per RF Domain. After 365 days, the oldest records (corresponding to the first day) are purged from B4. This expiration cycle is triggered every 1 day to enable B4 to maintain exactly 365 days worth of data.

### Example

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#nsight database statistics avc-update-interval 120
```

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#nsight database statistics update-interval 30
```

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#nsight database statistics wireless-clients-update-interval 600
```

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#nsight database statistics max-apps-per-
```

```
client 20
```

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#nsight database summary duration 12 30 200 500
```

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context include-factory | include nsight
use nsight-policy nsight-noc
nsight database statistics update-interval 30
nsight database statistics wireless-clients-update-interval 600
nsight database summary duration 12 30 200 500
nsight database statistics avc-update-interval 120
nsight database statistics max-apps-per-mu 20
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```

## Related Commands

|                              |                                                                             |
|------------------------------|-----------------------------------------------------------------------------|
| <code>no</code> on page 1271 | Reverts the NSight database related parameters configured to default values |
|------------------------------|-----------------------------------------------------------------------------|

*override-wlan*

[Device Config Commands](#) on page 1252

Configures WLAN's RF Domain level overrides

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
override-wlan <WLAN> [shutdown|ssid|vlan-pool|wep128|wpa-wpa2-psk]
```

```
override-wlan <WLAN> [shutdown|ssid <SSID>|vlan-pool <1-4094> {limit <0-8192>}]| wpa-wpa2-psk <WORD>]
```

```
override-wlan <WLAN> wep128 [key <1-4> hex [0<WORD>|2 <WORD>]]|transmit-key <1-4>]
```

### Parameters

```
override-wlan <WLAN> [shutdown|ssid <SSID>|vlan-pool <1-4094> {limit <0-8192>}]| wpa-wpa2-psk <WORD>]
```

|                          |                                                                                                                                          |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;WLAN&gt;</b>      | Specify the WLAN name.<br>Configure the following WLAN parameters: SSID, VLAN pool, and WPA-WPA2 key.                                    |
| <b>shutdown</b>          | Shuts down the WLAN's (identified by the <WLAN> keyword) operations on all mapped radios                                                 |
| <b>SSID &lt;SSID&gt;</b> | Configures the WLAN's Service Set Identifier (SSID) <ul style="list-style-type: none"><li>• &lt;SSID&gt; - Specify an SSID ID.</li></ul> |



|                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vlan-pool</b><br><b>&lt;1-4094&gt;</b><br><b>{limit</b><br><b>&lt;0-8192&gt;}</b> | Configures a pool of VLANs for the selected WLAN <ul style="list-style-type: none"> <li>• &lt;1-4094&gt; - Specifies a VLAN pool ID from 1 - 4094.</li> <li>• limit - Optional. Limits the number of users on this VLAN pool</li> <li>• &lt;0-8192&gt; - Specify the user limit from 0 - 8192.</li> </ul> <p style="text-align: center;"><b>Note:</b> The VLAN pool configuration overrides the VLAN configuration.</p> |
| <b>wpa-wpa2-psk</b><br><b>&lt;WORD&gt;</b>                                           | Configures the WLAN WPA-WPA2 key or passphrase for the selected WLAN <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specify a WPA-WPA2 key or passphrase.</li> </ul>                                                                                                                                                                                                                                           |

```
override-wlan <WLAN> wep128 [key <1-4> hex [0<WORD>|2 <WORD>]|transmit-key <1-4>]
```

|                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;WLAN&gt;</b>                                                                                                                            | Specify the WLAN name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>wep128 [key</b><br><b>&lt;1-4&gt; hex</b><br><b>[0&lt;WORD&gt;  2</b><br><b>&lt;WORD&gt;] </b><br><b>transmit-key</b><br><b>&lt;1-4&gt;</b> | Configures the WEP128 key for this WLAN, and also enables key transmission<br>Wired Equivalent Privacy (WEP) is a security protocol specified in the IEEE Wireless Fidelity (Wi-Fi) standard. WEP 128 uses a 104 bit key, which is concatenated with a 24-bit initialization vector (IV) to form the RC4 traffic key. This results in a level of security and privacy comparable to that of a wired LAN.                                                                                                                                                                                                                                                                                                                                      |
|                                                                                                                                                | <ul style="list-style-type: none"> <li>• key &lt;1-4&gt; hex - Configures a hexadecimal key (clear text or encrypted) and specifies the key's index. <ul style="list-style-type: none"> <li>• 0 &lt;WORD&gt; - Configures a clear text key. Specify a 4 - 32 character pass key.</li> <li>• 2 &lt;WORD&gt; - Configures an encrypted key. Specify a 4 - 32 character pass key.</li> </ul> </li> <li>• transmit-key &lt;1-4&gt; - Enables transmission of key index. Specify the key index.</li> </ul> <p>Wireless devices and their connected clients use the algorithm to convert an ASCII string to the same hexadecimal number. Clients without the required adapters need to use WEP keys manually configured as hexadecimal numbers.</p> |

### Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#override-wlan test vlan-pool 8
```

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
```

```
ap71xx 00-04-96-4A-A7-08
 use profile default-ap71xx
 use rf-domain default
 hostname TechPubAP7131
 floor 5thfloor
 layout-coordinates 1.0 2.0
 license AP aplicenseley@1234 aplicensekey@123
 location SanJose
 no contact
 country-code us
 channel-list 2.4GHz 1,2
 override-wlan test vlan-pool 8
 mac-name 00-04-96-4A-A7-08 5.8TestAP
 neighbor-info-interval 50
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

### Related Commands

|                        |                                        |
|------------------------|----------------------------------------|
| <b>no</b> on page 1271 | Removes RF Domain level WLAN overrides |
|------------------------|----------------------------------------|

## remove-override

[Device Config Commands](#) on page 1252

Removes device overrides in order to enable profile settings to take effect

### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

### Syntax

```
remove-override <PARAMETERS>
```

### Parameters

```
remove-override <PARAMETERS>
```

|                                                     |                                                                                                                                                                                       |
|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>remove-override</b><br><b>&lt;PARAMETERS&gt;</b> | Removes settings configured at the device level based on the parameters passed. The profile (applied to the device) settings take effect once the device-level overrides are removed. |
|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Example

```
rfs4000-229D58(config-device-00-23-68-22-9D-58)#remove-override ?
 adopter-auto-provisioning-policy-lookup Use centralized auto-provisioning
 policy when adopted by another
 controller
 adoption Adoption configuration
 adoption-mode Configure the adoption mode for the
 access-points in this RF-Domain
 alias Alias
 all Remove all overrides for the device
 application-policy Application Policy configuration
 area Reset name of area where the system
 is located
 arp Address Resolution Protocol (ARP)
 auto-learn Auto learning
 autogen-uniqueid Autogenerate a unique id
 autoinstall Autoinstall settings
 bridge Bridge group commands
 captive-portal Captive portal
 cdp Cisco Discovery Protocol
 channel-list Configure a channel list to be
 advertised to wireless clients
 cluster Cluster configuration
 configuration-persistence Automatic write of startup
 configuration file
 contact The contact
 controller WLAN controller configuration
 country-code The country of operation
 critical-resource Critical Resource
 crypto Encryption related commands
 device-upgrade Device firmware upgrade
 dot1x 802.1X
 dpi Deep-Packet-Inspection (Application
 Assurance)
```

|                             |                                                                                    |
|-----------------------------|------------------------------------------------------------------------------------|
| dscp-mapping                | IP DSCP to 802.1p priority mapping for untagged frames                             |
| email-notification          | Email notification configuration                                                   |
| enforce-version             | Check the firmware versions of devices before interoperating                       |
| environmental-sensor        | Environmental Sensors Configuration                                                |
| events                      | System event messages                                                              |
| export                      | Export a file                                                                      |
| file-sync                   | File sync between controller and adoptees                                          |
| firewall                    | Enable/Disable firewall                                                            |
| floor                       | Reset name of floor where the system is located                                    |
| geo-coordinates             | Geo co-ordinates for this device                                                   |
| global                      | Remove global overrides for the device but keeps per-interface overrides           |
| gre                         | GRE protocol                                                                       |
| interface                   | Select an interface to configure                                                   |
| ip                          | Internet Protocol (IP)                                                             |
| ipv6                        | Internet Protocol version 6 (IPv6)                                                 |
| l2tpv3                      | L2tpv3 protocol                                                                    |
| l3e-lite-table              | L3e lite Table                                                                     |
| led                         | LED on the device                                                                  |
| lldp                        | Link Layer Discovery Protocol                                                      |
| location                    | The location                                                                       |
| logging                     | Modify message logging facilities                                                  |
| mac-address-table           | MAC Address Table                                                                  |
| mac-auth                    | 802.1X                                                                             |
| memory-profile              | Memory-profile                                                                     |
| mint                        | MiNT protocol                                                                      |
| mpact-server                | MPACT server configuration                                                         |
| noc                         | Noc related configuration                                                          |
| ntp                         | Configure NTP                                                                      |
| offline-duration            | Duration to mark adopted device as offline                                         |
| override-wlan               | Overrides for wlangs                                                               |
| power-config                | Configure power mode                                                               |
| preferred-controller-group  | Controller group this system will prefer for adoption                              |
| preferred-tunnel-controller | Tunnel Controller Name this system will prefer for tunneling extended vlan traffic |
| rf-domain-manager           | RF Domain Manager                                                                  |
| router                      | Dynamic routing                                                                    |
| routing-policy              | Policy Based Routing Configuration                                                 |
| sensor-server               | AirDefense WIPS sensor server configuration                                        |
| spanning-tree               | Spanning tree                                                                      |
| timezone                    | The timezone                                                                       |
| traffic-class-mapping       | IPv6 traffic-class to 802.1p priority mapping for untagged frames                  |
| traffic-shape               | Traffic shaping                                                                    |
| trustpoint                  | Assign a trustpoint to a service                                                   |
| tunnel-controller           | Tunnel Controller group this controller belongs to                                 |
| use                         | Set setting to use                                                                 |
| vrrp                        | VRRP configuration                                                                 |
| service                     | Service Commands                                                                   |

rfs4000-229D58(config-device-00-23-68-22-9D-58)#

[Device Config Commands](#) on page 1252

Assigns an SSH RSA key

SSH keys are a pair of cryptographic keys used to authenticate users instead of, or in addition to, a username/password. One key is private and the other is public key. Secure Shell (SSH) public key authentication can be used by a requesting client to access resources, if properly configured. The RSA key pair must be generated on the client. The public portion of the key pair resides with the controller, service platform, or access point locally, while the private portion remains on a secure area of the client.

#### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
rsa-key ssh <RSA-KEY-NAME>
```

#### Parameters

```
rsa-key ssh <RSA-KEY-NAME>
```

|                             |                                                                                                                                                                         |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>rsa-key ssh</b>          | Assigns RSA key to SSH                                                                                                                                                  |
| <b>&lt;RSA-KEY-NAME&gt;</b> | <ul style="list-style-type: none"><li>• &lt;RSA-KEY-NAME&gt; - Specifies the RSA key name. The key should be installed using PKI commands in the enable mode.</li></ul> |

#### Example

```
nx9500-6C8809(config-device-00-04-96-4A-A7-08)#rsa-key ssh rsa-key1
```

```
nx9500-6C8809(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
 use profile default-ap71xx
 use rf-domain default
 hostname TechPubAP7161
 floor 5thfloor
 layout-coordinates 1.0 2.0
 license AP aplicenseley@1234 aplicensekey@123
 rsa-key ssh rsa-key1
 location SanJose
 no contact
 country-code us
 channel-list 2.4GHz 1,2
 override-wlan test vlan-pool 8
 mac-name 00-04-96-4A-A7-08 5.8TestAP
 neighbor-info-interval 50
nx9500-6C8809(config-device-00-04-96-4A-A7-08)#
```

#### Related Commands

|                        |                              |
|------------------------|------------------------------|
| <b>no</b> on page 1271 | Removes RSA key from service |
|------------------------|------------------------------|

[Device Config Commands](#) on page 1252

Configures an AirDefense sensor server resource for client terminations and WIPS event logging. This is the server that supports WIPS events on behalf of the controller or service platform.

**Supported in the following platforms:**

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
sensor-server <1-3> ip <IP/HOSTNAME> {port [443|<1-65535>]}
```

**Parameters**

```
sensor-server <1-3> ip <IP/HOSTNAME> {port [443|<1-65535>]}
```

|                                            |                                                                                                                                                                                                                                                                                        |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>sensor-server</b><br><b>&lt;1-3&gt;</b> | Sets a numerical index to differentiate this AirDefense sensor server from other servers. A maximum of 3 (three) sensor server resources can be defined.                                                                                                                               |
| <b>ip &lt;IP/<br/>HOSTNAME&gt;</b>         | Configures the AirDefense sensor server's IP address or hostname <ul style="list-style-type: none"><li>• &lt;IP/HOSTNAME&gt; - Specify the IP address.</li></ul>                                                                                                                       |
| <b>port [443  <br/>&lt;1-65535&gt;]</b>    | Optional. Configures the port. The options are: <ul style="list-style-type: none"><li>• 443 - The default port used by the AirDefense server. This is the default setting.</li><li>• &lt;1-65535&gt; - Manually sets the port number of the AirDefense server from 1 - 65535</li></ul> |

**Example**

```
nx9500-6C8809(config-device-00-04-96-4A-A7-08)#sensor-server 1 ip 172.16.10.7

nx9500-6C8809(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
 use profile default-ap71xx
 use rf-domain default
 hostname TechPubAP7161
 floor 5thfloor
 layout-coordinates 1.0 2.0
 license AP aplicenseley@1234 aplicensekey@123
 rsa-key ssh rsa-key1
 location SanJose
 no contact
 country-code us
 sensor-server 1 ip 172.16.10.7
 channel-list 2.4GHz 1,2
 override-wlan test vlan-pool 8
 mac-name 00-04-96-4A-A7-08 5.8TestAP
 neighbor-info-interval 50
nx9500-6C8809(config-device-00-04-96-4A-A7-08)#
```

**Related Commands**

|                                 |                                           |
|---------------------------------|-------------------------------------------|
| <a href="#">no</a> on page 1271 | Removes configured sensor server settings |
|---------------------------------|-------------------------------------------|

*timezone*

[Device Config Commands](#) on page 1252

Configures device's timezone

**Supported in the following platforms:**

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

**Syntax**

```
timezone <TIMEZONE>
```

**Parameters**

```
timezone <TIMEZONE>
```

|                                            |                                  |
|--------------------------------------------|----------------------------------|
| <b>timezone</b><br><b>&lt;TIMEZONE&gt;</b> | Configures the device's timezone |
|--------------------------------------------|----------------------------------|

**Example**

```
nx9500-6C8809(config-device-00-04-96-4A-A7-08)#timezone Etc/UTC

nx9500-6C8809(config-device-00-04-96-4A-A7-08)#show context
ap7lxx 00-04-96-4A-A7-08
 use profile default-ap7lxx
 use rf-domain default
 hostname TechPubAP7161
 floor 5thfloor
 layout-coordinates 1.0 2.0
 license AP aplicenseley@1234 aplicensekey@123
 rsa-key ssh rsa-key1
 location SanJose
 no contact
 timezone Etc/UTC
 stats open-window 2 sample-interval 77 size 10
 country-code us
 sensor-server 1 ip 172.16.10.7
 channel-list 2.4GHz 1,2
 override-wlan test vlan-pool 8
 mac-name 00-04-96-4A-A7-08 5.8TestAP
 neighbor-info-interval 50
nx9500-6C8809(config-device-00-04-96-4A-A7-08)#
```

**Related Commands**

|                                 |                                      |
|---------------------------------|--------------------------------------|
| <a href="#">no</a> on page 1271 | Removes device's configured timezone |
|---------------------------------|--------------------------------------|

*trustpoint (device-config-mode)*

[Device Config Commands](#) on page 1252

Assigns trustpoints to validate various services, such as HTTPS, RADIUS CA, RADIUS server, external LDAP server, etc.

For more information on digital certificates and certificate authorities, see [trustpoint \(profile-config-mode\)](#) on page 1229.



#### Note

Certificates/trustpoints used in this command should be verifiable as existing on the device.

#### Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

#### Syntax

```
trustpoint [cloud-client | cmp-auth-operator | https | radius-ca | radius-ca-ldaps | radius-server | radius-server-ldaps] <TRUSTPOINT-NAME>
```

#### Parameters

```
trustpoint [cloud-client | cmp-auth-operator | https | radius-ca | radius-ca-ldaps | radius-server | radius-server-ldaps] <TRUSTPOINT-NAME>
```

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>trustpoint</b>        | Assigns trustpoints to validate various services. The assigned trustpoint is used as the CA for validating the services.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>cloud-client</b>      | Assigns trustpoint to validate cloud client. The trustpoint should be existing and installed on the device.<br>Use this option on cloud-enabled access points and cloud-adopted, to secure the communication between the cloud AP and cloud client. The trustpoint should be existing and installed on the AP. The cloud-enabled access points are AP7502, AP7522, AP7532, and AP7562. For local-controller adopted APs, this configuration is not required.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>cmp-auth-operator</b> | Assigns an existing trustpoint to validate CMP auth operator. Once validated, CMP is used to obtain and manage digital certificates in a PKI network. Digital certificates link identity information with a public key enclosed within the certificate, and are issued by the CA.<br>Use this command to specify the CMP-assigned trustpoint. When specified, devices send a certificate request to the CMP supported CA server, and download the certificate directly from the CA server. CMP supports multiple request options through for device communicating to a CMP supported CA server. The device can initiate a request for getting the certificates from the server. It can also auto update the certificates which are about to expire.<br><br><b>Note:</b> When configured, this cmp-auth-operator trustpoint setting overrides the profile-level configuration. |
| <b>https</b>             | Assigns an existing trustpoint to validate HTTPS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>radius-ca</b>         | Assigns an existing trustpoint to validate client certificates in EAP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>radius-ca-ldaps</b>   | Assigns an existing trustpoint to validate external LDAP server                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>radius-server</b>     | Assigns an existing trustpoint to validate RADIUS server certificate                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>radius-server-ldaps</b>     | Assigns an existing trustpoint to RADIUS server certificate to validate LDAP server                                                                                                                                                                                                                                                                                                                                          |
| <b>&lt;TRUSTPOINT-NAME&gt;</b> | <p>The following keyword is common to all of the above parameters:</p> <ul style="list-style-type: none"> <li>• &lt;TRUSTPOINT-NAME&gt; – After selecting the service to validate, specify the trustpoint name (should be existing and stored on the device).</li> </ul> <p><b>Note:</b> By default, the system assigns the default-trustpoint to validate the following: https, radius-server, and radius-server-ldaps.</p> |

### Example

A device's default HTTPS, RADIUS, and CMP certificate/trustpoint configuration is as follows:

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context include-factory | include trustpoint
trustpoint https default-trustpoint
no trustpoint radius-ca
trustpoint radius-server default-trustpoint
no trustpoint radius-ca-ldaps
trustpoint radius-server-ldaps default-trustpoint
no trustpoint cmp-auth-operator
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#trustpoint https test
```

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context include-factory | include trustpoint
trustpoint https test
no trustpoint radius-ca
trustpoint radius-server default-trustpoint
no trustpoint radius-ca-ldaps
trustpoint radius-server-ldaps default-trustpoint
no trustpoint cmp-auth-operator
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```

*raid*

[Device Config Commands](#) on page 1252

Enables chassis alarm that sounds when events are detected that degrade RAID support (drive content mirroring) on a service platform

The NX95XX (NX9500 and NX9510) series service platforms include a single Intel MegaRAID controller (virtual drive) with RAID-1 mirroring support enabled. The online virtual drive supports up to two physical drives that could require hot spare substitution if a drive were to fail. The WiNG software allows you to manage the RAID controller event alarm and syslogs supporting the array hardware from the service platform user interface without rebooting the service platform BIOS.

Although RAID controller drive arrays are available only on the NX95XX series service platforms, they can be administrated on behalf of a NX95XX profile by a different model service platform or wireless controller.

#### Supported in the following platforms:

- Service Platforms — NX7530, NX9500, NX9510, NX9600



## Syntax

```
raid alarm enable
```

## Parameters

```
raid alarm enable
```

|                     |                                                                                                                                                                                                 |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>alarm enable</b> | Enables audible alarm, which is triggered a RAID drives fails. When triggered the alarm can be disabled by executing the <code>raid &gt; silence</code> command in the device's Priv Exec mode. |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Example

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#raid alarm enable
```

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context
```

```
nx9000 B4-C7-99-6C-88-09
 use profile default-nx9000
 use rf-domain default
 hostname nx9500-6C8809
 ip default-gateway 192.168.13.2
 interface gel
 switchport mode access
 switchport access vlan 1
 interface vlan1
 ip address 192.168.13.13/24
 logging on
 logging console warnings
 logging buffered warnings
 raid alarm enable
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```

## Related Commands

|                        |                     |
|------------------------|---------------------|
| <b>no</b> on page 1200 | Disables RAID alarm |
|------------------------|---------------------|

## T5 Profile Config Commands

[PROFILES](#) on page 857

A T5 controller uses the IPX operating system to manage its connected radio devices, as opposed to the WiNG operating used by RFS wireless controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The Customer Premises Equipment (CPEs) are the T5 controller managed radio devices using the IPX operating system. These CPEs use a DSL as their high speed Internet access mechanism using the CPE's physical wallplate connection and phone jack.

To navigate to this instance, use the following commands:

```
<DEVICE>(config-profile-<PROFILE-NAME>)#?
T5 Profile Mode commands:
 cpe T5 CPE configuration
 interface Select an interface to configure
 ip Internet Protocol (IP)
 no Negate a command or set its defaults
 ntp Configure NTP
 override-wlan Configure RF Domain level overrides for wlan
```

```

t5 T5 configuration
t5-logging Modify message logging facilities
use Set setting to use

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

```

<DEVICE>(config-profile-<PROFILE-NAME>)#

The following table summarizes T5 profile configuration mode commands:

| Command                                    | Description                                                                                                         |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| <a href="#">cpe</a> on page 1286           | Configures T5 CPE related settings (IP address range and VLAN)                                                      |
| <a href="#">interface</a> on page 1288     | Configures the T5 controller's interfaces                                                                           |
| <a href="#">ip</a> on page 1290            | Configures the default gateway's IP address                                                                         |
| <a href="#">no</a> on page 1291            | Removes or reverts this T5 controller profile settings                                                              |
| <a href="#">ntp</a> on page 1292           | Configures the NTP server associated with this T5 profile                                                           |
| <a href="#">override-wlan</a> on page 1293 | Configures the RF Domain level overrides for applied on a WLAN on this T5 profile                                   |
| <a href="#">t5</a> on page 1294            | Configures the logged T5 controller's country of operation                                                          |
| <a href="#">t5-logging</a> on page 1294    | Configures a maximum of 5 (five) remote hosts capable of receiving syslog messages from this selected T5 controller |
| <a href="#">use</a> on page 1295           | Defines this T5 profile's management settings                                                                       |

## *cpe*

[T5 Profile Config Commands](#) on page 1285

Configures T5 CPE related settings. This command is available both in the T5 profile and T5 device contexts

### **Supported in the following platforms:**

- Wireless Controllers — RFS4000
- Service Platforms — NX9500, NX9510

### **Syntax T5 Profile & T5 Device Context**

```
cpe [address led]
```

```
cpe address vlan <1-4094> <START-IP> <END-IP>
```

```
cpe led cpe <cpe1-24>
```

The following commands are specific to the T5 device context:

```
cpe [boot|reload|upgrade]
```

```
cpe boot system <cpe1-24> <primary|secondary>
```

```
cpe reload <cpe1-24>
```

```
cpe <cpe1-24> upgrade <IMAGE-LOCATION>
```

### Parameters

```
cpe address vlan <1-4094> <START-IP> <END-IP>
```

|                                            |                                                                                                                                                                                                                                                                                          |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>cpe address</b>                         | Configures the range of addresses that can be assigned to adopted CPEs                                                                                                                                                                                                                   |
| <b>vlan &lt;1-4094&gt;</b>                 | Configures the VLAN assigned to the CPEs managed by this T5 controller                                                                                                                                                                                                                   |
| <b>&lt;START-IP&gt;<br/>&lt;END-IP&gt;</b> | Configures the range of IP addresses that can be assigned to the CPEs managed by this T5 controller <ul style="list-style-type: none"><li>• &lt;START-IP&gt; - Specify the first IP address in the range.</li><li>• &lt;END-IP&gt; - Specify the last IP address in the range.</li></ul> |

```
cpe led cpe <cpe1-24>
```

|                            |                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>cpe led</b>             | Enables flashing of LEDs on specified CPEs                                                                                                                                                                                                                                                                                                                                       |
| <b>cpe &lt;cpe1-24&gt;</b> | Identifies the CPE(s) on which the operation is performed <ul style="list-style-type: none"><li>• &lt;cpe1-24&gt; - Configures the CPE's ID from cpe1 - cpe24. To enable led flashing on all adopted CPEs, enter cpe1-X, where X is the total number of adopted CPEs. For example, if CPEs 1, 2, 3, 4, &amp; 5 are adopted and ready, then enter this value as cpe1-5.</li></ul> |

```
cpe boot system <cpe1-24> <primary|secondary>
```

|                                  |                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>• cpe boot system</b>         | Changes the image used by a CPE to boot. When reloading, the CPE uses the specified image.                                                                                                                                                                                                                                                                                       |
| <b>&lt;cpe1-24&gt;</b>           | Identifies the CPE(s) on which the operation is performed <ul style="list-style-type: none"><li>• &lt;cpe1-24&gt; - Configures the CPE's ID from cpe1 - cpe24. To enable led flashing on all adopted CPEs, enter cpe1-X, where X is the total number of adopted CPEs. For example, if CPEs 1, 2, 3, 4, &amp; 5 are adopted and ready, then enter this value as cpe1-5.</li></ul> |
| <b>&lt;primary secondary&gt;</b> | Select the next boot image <ul style="list-style-type: none"><li>• primary - Uses the primary image when reloading</li><li>• secondary - Uses the secondary image when reloading</li></ul>                                                                                                                                                                                       |

```
cpe reload <cpe1-24>
```

|                        |                                                                                                                                                                                                                                                                                                                                                          |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>cpe reload</b>      | Reloads all or specified CPEs.                                                                                                                                                                                                                                                                                                                           |
| <b>&lt;cpe1-24&gt;</b> | Identifies the CPE(s) to reload <ul style="list-style-type: none"> <li>• &lt;cpe1-24&gt; - Configures the CPE's ID from cpe1 - cpe24. To enable led flashing on all adopted CPEs, enter cpe1-X, where X is the total number of adopted CPEs. For example, if CPEs 1, 2, 3, 4, &amp; 5 are adopted and ready, then enter this value as cpe1-5.</li> </ul> |

```
cpe <cpe1-24> upgrade <IMAGE-LOCATION>
```

|                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>cpe &lt;cpe1-24&gt;</b>            | Upgrades all or specified CPEs                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>upgrade &lt;IMAGE-LOCATION&gt;</b> | <ul style="list-style-type: none"> <li>• &lt;cpe1-24&gt; - Identifies the CPE(s) to upgrade. Specify the CPE's ID from cpe1 - cpe24. To enable led flashing on all adopted CPEs, enter cpe1-X, where X is the total number of adopted CPEs. For example, if CPEs 1, 2, 3, 4, &amp; 5 are adopted and ready, then enter this value as cpe1-5.</li> <li>• upgrade &lt;IMAGE-LOCATION&gt; - Uses the image specified here to upgrade identified CEPS. <ul style="list-style-type: none"> <li>&lt;IMAGE-LOCATION&gt; - Specify the firmware image location using one of the following options: <pre>path/file</pre> <pre>tftp://&lt;IP&gt;/path/file</pre> <pre>ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;IP&gt;/path/file</pre> </li> </ul> </li> </ul> |

### Example

```
nx9500-6C8809(config-profile-T5TestProfile)#cpe address vlan 200 192.168.13.26
192.168.13.30
```

```
nx9500-6C8809(config-profile-T5TestProfile)#show context
profile t5 T5TestProfile
no autoinstall configuration
no autoinstall firmware
interface vlan1
interface vlan4090
interface fe 5 2
.....
interface radio 11 1
interface fe 9 2
interface radio 18 1
interface fe 9 1
use firewall-policy default
service pm sys-restart
cpe address vlan 200 192.168.13.26 192.168.13.30
nx9500-6C8809(config-profile-T5TestProfile)#
```

### interface

[T5 Profile Config Commands](#) on page 1285

Configures the T5 controller's interfaces

### Supported in the following platforms:

- Wireless Controllers — RFS4000
- Service Platforms — NX9500, NX9510

## Syntax

```
interface [<WORD>|dsl|fe|ge|radio|vlan]
```

```
interface [<WORD>|dsl <1-24>|fe <1-24> <1-2>|ge <1-2>|radio <1-24> <1-2>|
vlan <1-4094>]
```

## Parameters

```
interface [<WORD>|dsl <1-24>|fe <1-24> <1-2>|ge <1-2>|radio <1-24> <1-2>|vlan <1-4094>]
```

|                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;WORD&gt;</b>                       | Configures the interface identified by the <WORD> keyword                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>dsl &lt;1-24&gt;</b>                   | <p>Configures the specified DSL interface. A T5 controller uses the IPX operating system to manage its connected radio devices, as opposed to the WiNG operating used by controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The CPEs are the T5 controller managed radio devices using the IPX operating system. These CPEs use DSL as their high speed Internet access mechanism using the CPE's physical wallplate connection and phone jack.</p> <ul style="list-style-type: none"><li>• &lt;1-24&gt; – Specify the DSL port index from 1 - 24.</li></ul>                                                   |
| <b>fe &lt;1-24&gt;<br/>&lt;1-2&gt;</b>    | <p>Configures the specified FastEthernet interface. The T5 controller has the following FastEthernet port designations: fe1-fe2 (fe1-fe2 are for up to 24 CPE devices managed by a T5 controller).</p> <ul style="list-style-type: none"><li>• &lt;1-24&gt; – Specify the DSL port index from 1 - 24.</li><li>• &lt;1-2&gt; – Specify the FastEthernet interface to configure.</li></ul> <p>In the FastEthernet interface configuration mode, specify the interface settings.</p>                                                                                                                                                                                                                                                                                                                   |
| <b>ge &lt;1-2&gt;</b>                     | <p>Configures the specified GigabitEthernet interface. T5 controllers have two Ethernet port designations, These are ge1 and ge2. The GE ports can be RJ-45 or fiber ports supporting 10/100/1000Mbps.</p> <ul style="list-style-type: none"><li>• &lt;1-2&gt; – Specify the interface index from 1 - 2.</li></ul> <p>In the GigabitEthernet interface configuration mode, specify the interface settings.</p>                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>radio &lt;1-24&gt;<br/>&lt;1-2&gt;</b> | <p>Configures the specified radio interface. T5 controller managed CPE device radios can have their radio configurations overridden once their radios have successfully associated and have been provisioned by the adopting controller, service platform, or peer model AP controller access point.</p> <ul style="list-style-type: none"><li>• &lt;1-24&gt; – Specify the radio interface index from 1 - 24.</li><li>• &lt;1-2&gt; – Allows the second radio to be specified as a radio interface. For example, this is “interface radio X Y” where ‘X’ is the DSL line number and ‘Y’ is the radio interface (number).</li></ul>                                                                                                                                                                 |
| <b>vlan &lt;1-4094&gt;</b>                | <p>Configures the specified VLAN interface. Once configured, the VLAN interface provides layer 3 (IP) T5 controller access or provides layer 3 service on a VLAN. The VLAN interface defines which IP address is associated with each VLAN ID a T5 controller is connected to. A VLAN interface is created for the default VLAN (VLAN 1) to enable remote administration. This interface is also used to map VLANs to IP4 and IPv6 formatted IP address ranges. This mapping determines the destination for routing.</p> <ul style="list-style-type: none"><li>• &lt;1-4094&gt; – Specify the VLAN interface index from 1 - 4094.</li></ul> <p>In the VLAN configuration mode, specify the interface's primary IP address in the A.B.C.D/M format. Optionally specify the secondary IP address.</p> |

## Example

```
rfs7000-37FABE(config-profile-t5Profile)#interface dsl 1

rfs7000-37FABE(config-profile-t5Profile-if-dsl1)#?
Interface configuration commands:
 description Port description
 ds-interleaver Enable impulse noise protection in the downstream
 direction
 ds-max-datarate Configure maximum allowed downstream rate for the
 interface
 ds-min-margin Configure the minimum downstream signal-to-noise(SNR)
 ratio margin
 ds-target-margin Configure the desired downstream signal-to-noise (SNR)
 ratio margin
 duplex Set duplex to interface
 flowcontrol Set flowcontrol to interface
 line-power Use the line-power command to apply power to the interface
 no Negate a command or set its defaults
 qos QOS settings
 shutdown Shutdown the selected interface
 speed Configure speed
 switchport Set switching mode characteristics
 us-interleaver Enable impulse noise protection in the upstream direction
 us-max-datarate Configure maximum allowed upstream rate for the interface
 us-min-margin Configure the minimum upstream signal-to-noise (SNR) ratio
 margin
 us-target-margin Configure the desired upstream signal-to-noise (SNR) ratio
 margin

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
--More--
rfs7000-37FABE(config-profile-t5Profile-if-dsl1)#
```

## Related Commands

|                                 |                                                               |
|---------------------------------|---------------------------------------------------------------|
| <a href="#">no</a> on page 1291 | Removes the selected interface configuration on the T5 device |
|---------------------------------|---------------------------------------------------------------|

*ip*

[T5 Profile Config Commands](#) on page 1285

Configures the default gateway's IP address

### Supported in the following platforms:

- Wireless Controllers — RFS4000
- Service Platforms — NX9500, NX9510

### Syntax

```
ip default-gateway <IP>
```

## Parameters

```
ip default-gateway <IP>
```

|                                      |                                                               |
|--------------------------------------|---------------------------------------------------------------|
| <b>ip default-gateway &lt;IP&gt;</b> | Enter the default gateway's IP address in the A.B.C.D format. |
|--------------------------------------|---------------------------------------------------------------|

## Example

```
nx9500-6C8809(config-profile-t5Profile)#ip default-gateway 192.168.13.7
```

```
nx9500-6C8809(config-profile-t5Profile)#show context
profile t5 t5Profile
```

```
 ip default-gateway 192.168.13.7
 no autoinstall configuration
 no autoinstall firmware
 interface vlan1
 interface vlan4090
 interface fe 5 2
 interface ge 2
 interface ge 1
 interface fe 5 1
```

```
--More--
```

```
nx9500-6C8809(config-profile-t5Profile)#
```

*no*

[T5 Profile Config Commands](#) on page 1285

Removes or reverts this T5 controller profile settings

### Supported in the following platforms:

- Wireless Controllers — RFS4000
- Service Platforms — NX9500, NX9510

## Syntax

```
no [cpe|interface|ntp|override-wlan|t5-logging|use]
```

```
no cpe led cpe <1-24>
```

```
no interface vlan <2-4094>
```

```
no ntp server <IP>
```

```
no override-wlan <WLAN-NAME> vlan
```

```
no t5-logging host <IP>
```

```
no use management-policy
```

## Parameters

```
no <PARAMETERS>
```

|                                        |                                                                              |
|----------------------------------------|------------------------------------------------------------------------------|
| <b>no</b><br><b>&lt;PARAMETERS&gt;</b> | Removes or reverts to default the selected T5 profile's or device's settings |
|----------------------------------------|------------------------------------------------------------------------------|

## Example

```
nx9500-6C8809(config-profile-t5Profile)#show context
profile t5 t5Profile
 ip default-gateway 192.168.13.7
 no autoinstall configuration
 no autoinstall firmware
 interface vlan1
 interface vlan4090

 use firewall-policy default
 ntp server 192.168.13.2
 service pm sys-restart
nx9500-6C8809(config-profile-t5Profile)#

nx9500-6C8809(config-profile-t5Profile)#no ntp server 192.168.13.2

nx9500-6C8809(config-profile-t5Profile)#show context
profile t5 t5Profile
 ip default-gateway 192.168.13.7
 no autoinstall configuration
 no autoinstall firmware
 interface vlan1
 interface vlan4090

 use firewall-policy default
 service pm sys-restart
nx9500-6C8809(config-profile-t5Profile)#
```

*ntp*

[T5 Profile Config Commands](#) on page 1285

Configures the NTP server associated with this T5 profile. T5 controllers, using this profile, will obtain their system time from the specified NTP server resources.

### Supported in the following platforms:

- Wireless Controllers — RFS4000
- Service Platforms — NX9500, NX9510

### Syntax

```
ntp server <IP>
```

### Parameters

```
ntp server <IP>
```

|                                        |                                                                                                   |
|----------------------------------------|---------------------------------------------------------------------------------------------------|
| <b>ntp server</b><br><b>&lt;IP&gt;</b> | Specify the NTP server's IP address. You can specify a maximum of 3 (three) NTP server resources. |
|----------------------------------------|---------------------------------------------------------------------------------------------------|

### Example

```
nx9500-6C8809(config-profile-t5Profile)#ntp server 192.168.13.2

nx9500-6C8809(config-profile-t5Profile)#show context
profile t5 t5Profile
 ip default-gateway 192.168.13.7
 no autoinstall configuration
 no autoinstall firmware
 interface dsl 5
```



```

.....
use firewall-policy default
ntp server 192.168.13.2
service pm sys-restart
nx9500-6C8809(config-profile-t5Profile)#

```

### Related Commands

|                              |                                     |
|------------------------------|-------------------------------------|
| <code>no</code> on page 1291 | Removes the NTP server's IP address |
|------------------------------|-------------------------------------|

### *override-wlan*

[T5 Profile Config Commands](#) on page 1285

Use this option to configure RF Domain level configuration for WLAN. The override configured here are applied to all T5 devices using this T5 profile.

#### Supported in the following platforms:

- Wireless Controllers – RFS4000
- Service Platforms – NX9500, NX9510

#### Syntax

```
override-wlan <WLAN-NAME> vlan <1-4094>
```

#### Parameters

```
override-wlan <WLAN-NAME> vlan <1-4094>
```

|                                        |                                                                                                              |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------|
| <b>override-wlan &lt;WLAN-NAME&gt;</b> | <b>Note:</b> Overrides the specified WLAN's VLAN configuration<br><br><WLAN-NAME> - Specify the WLAN's name. |
| <b>vlan &lt;1-4094&gt;</b>             | Specify the new VLAN option<br>• <1-4094> - Specify the VLAN from 1 - 4094.                                  |

#### Example

The following example displays the WLAN SJOFFWLAN configuration:

```

nx9500-6C8809(config-wlan-SJOFFWLAN)#show context
wlan SJOFFWLAN
description "SJ Office WLAN"
ssid SJOFFWLAN
vlan 468
bridging-mode local
encryption-type ccmp
authentication-type eap-psk
use aaa-policy test
nx9500-6C8809(config-wlan-SJOFFWLAN)#

```

The following example overrides the SJOFFWLAN WLAN's VLAN configuration on the T5 profile:

```

nx9500-6C8809(config-profile-testT5)#override-wlan SJOFFWLAN vlan 30

nx9500-6C8809(config-profile-testT5)#show context include-factory | include override-wlan
override-wlan SJOFFWLAN vlan 30
nx9500-6C8809(config-profile-testT5)#

```

## Related Commands

|                              |                                                                                |
|------------------------------|--------------------------------------------------------------------------------|
| <code>no</code> on page 1291 | Removes the RF Domain level overrides for applied on a WLAN on this T5 profile |
|------------------------------|--------------------------------------------------------------------------------|

*t5*

[T5 Profile Config Commands](#) on page 1285

Configures this T5 controller's country of operation

### Supported in the following platforms:

- Wireless Controllers — RFS4000
- Service Platforms — NX9500, NX9510

### Syntax

```
t5 country-code <WORD>
```

### Parameters

```
t5 country-code <WORD>
```

|                                            |                                                                      |
|--------------------------------------------|----------------------------------------------------------------------|
| <b>country-code</b><br><b>&lt;WORD&gt;</b> | Configures the 2 letter ISO-3166 country code for this T5 controller |
|--------------------------------------------|----------------------------------------------------------------------|

### Example

```
nx9500-6C8809(config-profile-T5TestProfile)#t5 country-code us
```

```
nx9500-6C8809(config-profile-T5TestProfile)#show context
profile t5 T5TestProfile
 no autoinstall configuration
 no autoinstall firmware
 interface vlan1
 interface vlan4090
 interface fe 5 2

 interface fe 9 1
 use firewall-policy default
 service pm sys-restart
 t5 country-code US
 cpe address vlan 200 192.168.13.26 192.168.13.30
nx9500-6C8809(config-profile-T5TestProfile)#
```

*t5-logging*

[T5 Profile Config Commands](#) on page 1285

Configures a maximum of 5 (five) remote hosts capable of receiving syslog messages from this selected T5 controller

### Supported in the following platforms:

- Wireless Controllers — RFS4000
- Service Platforms — NX9500, NX9510

## Syntax

```
t5-logging host <IP> severity [error|info|notice|trace|warning] facility
[local0|local1|local2|local3|local4|local5|local6|local7]
```

## Parameters

```
t5-logging host <IP> severity [error|info|notice|trace|warning] facility [local0|local1|
local2|local3|local4|local5|local6|local7]
```

|                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>t5-logging</b><br><b>host &lt;IP&gt;</b>                                                                                                | Configures syslog message logging settings <ul style="list-style-type: none"><li>host &lt;IP&gt; – Configures the external syslog remote host resource's IP address. This is the host dedicated to receive T5 syslog messages.</li></ul>                                                                                                                                                                                                                                                                                                                              |
| <b>severity</b><br><b>[error info </b><br><b>notice  trace </b><br><b>warning]</b>                                                         | Configures the syslog message filtering severity level. The options are: <ul style="list-style-type: none"><li>Error – Only forwards error and above syslog event messages.</li><li>Info – Only forwards informational and above syslog event messages.</li><li>notice – Only forwards syslog notices relating to general device operational events. These are events that are of more interest than the “info” events.</li><li>trace – Only forwards trace routing event messages</li><li>warning – Only forwards warnings and above syslog event messages</li></ul> |
| <b>facility</b><br><b>[local0 </b><br><b>local1 </b><br><b>local2 local3 </b><br><b>local4 </b><br><b>local5 local6 </b><br><b>local7]</b> | Configures the facility level for log messages sent to the syslog server. The facility level specifies the type of program logging the message. Specifying the facility level allows the configuration file to specify that message handling will vary with varying facility type. The options are: local0, local1, local2, local3, local4, local5, local5, local6, local7. The default value is local7.                                                                                                                                                              |

## Example

```
nx9500-6C8809(config-profile-T5TestProfile)#t5-logging host 192.168.13.10 severity warning
facility local6
```

```
nx9500-6C8809(config-profile-T5TestProfile)#show context
profile t5 T5TestProfile
t5-logging host 192.168.13.10 severity warning facility local6
no autoinstall configuration
.....
no autoinstall firmware
t5 country-code US
cpe address vlan 200 192.168.13.26 192.168.13.30
nx9500-6C8809(config-profile-T5TestProfile)#
```

## Related Commands

|                                 |                                                        |
|---------------------------------|--------------------------------------------------------|
| <a href="#">no</a> on page 1291 | Modifies message logging severity level and facilities |
|---------------------------------|--------------------------------------------------------|

use

[T5 Profile Config Commands](#) on page 1285

Associates a management policy with this T5 profile. The specified policy is applied to all T5 controllers using this profile.

### Supported in the following platforms:

- Wireless Controllers — RFS4000
- Service Platforms — NX9500, NX9510

### Syntax

```
use management-policy <POLICY-NAME>
```

### Parameters

```
use management-policy <POLICY-NAME>
```

|                            |                                                                                                               |
|----------------------------|---------------------------------------------------------------------------------------------------------------|
| <b>use</b>                 | Associates a management policy with this T5 profile (should be existing and configured)                       |
| <b>management-policy</b>   | <ul style="list-style-type: none"><li>• &lt;POLICY-NAME&gt; - Specify the management policy's name.</li></ul> |
| <b>&lt;POLICY-NAME&gt;</b> |                                                                                                               |

### Example

```
nx9500-6C8809(config-profile-t5Profile)#use management-policy default
Trustpoints HTTPS Server and RSA keys for SSH can be configured with 'trustpoint' and
'rsa-key' commands in device context
nx9500-6C8809(config-profile-t5Profile)#
```

### Related Commands

|                        |                                                         |
|------------------------|---------------------------------------------------------|
| <b>no</b> on page 1291 | Removes the management policy used with this T5 profile |
|------------------------|---------------------------------------------------------|

## EX3524 & EX3548 Profile/Device Config Commands

**PROFILES** on page 857

Creates a new EX3524 and EX3548 profile and enters its configuration mode.

To navigate to this instance, use the following commands:

```
<DEVICE>(config)#profile ex35xx <EX35XX-PROFILE-NAME>
```

Where ex35xx can be a EX3524 or a EX3548 device type.

```
<DEVICE>(config-profile-<EX35XX-PROFILE-NAME>)#?
EX35XX Profile Mode commands:
 interface Select an interface to configure
 ip Internet Protocol (IP)
 no Negate a command or set its defaults
 power EX3500 Power over Ethernet Command
 upgrade Configures upgrade option for ex3500 system
 use Set setting to use

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal
```

```
<DEVICE>(config-profile-<EX35XX-PROFILE-NAME>)#
```

The following table summarizes EX3524 and EX3548 profile/device configuration mode commands:

| Command                                | Description                                                                             |
|----------------------------------------|-----------------------------------------------------------------------------------------|
| <a href="#">interface</a> on page 1297 | Selects an interface type and enters the selected interface's configuration mode        |
| <a href="#">ip</a> on page 1310        | Configures the default gateway through which this EX35XX switch can reach other subnets |
| <a href="#">power</a> on page 1311     | Enables power inline compatibility mode on this EX35XX profile                          |
| <a href="#">upgrade</a> on page 1312   | Configures adopted EX35XX switch upgrade settings                                       |
| <a href="#">use</a> on page 1313       | Applies an EX3500 management policy to this EX35XX profile                              |
| <a href="#">no</a> on page 1314        | Removes or reverts this EX35XX profile's settings                                       |

## *interface*

[EX3524 & EX3548 Profile/Device Config Commands](#) on page 1296

This command selects an interface type and enters the selected interface's configuration mode. The EX35XX switch has GE and VLAN interfaces. Select the interface type and provide the interface ID to enter its configuration mode.

| Command                                                     | Description                                                                      |
|-------------------------------------------------------------|----------------------------------------------------------------------------------|
| <a href="#">interface</a> on page 1297                      | Selects an interface type and enters the selected interface's configuration mode |
| <a href="#">interface-ge-config commands</a> on page 1299   | Summarizes GE interface configuration mode commands                              |
| <a href="#">interface-vlan-config commands</a> on page 1308 | Summarizes VLAN interface configuration mode commands                            |

## **interface**

[interface](#) on page 1297

Selects the EX35XX interface type and enters the selected interface's configuration mode

Supported in the following platforms:

- Switches — EX3524, EX3548
- Wireless Controllers — RFS4000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
interface [ge 1 <1-48>|vlan <1-4094>]
```

Parameters

```
interface [ge 1 <1-48>|vlan <1-4094>]
```

|                            |                                                                                                                                                                                                                                                                                                                                     |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>interface</b>           | Selects the EX35XX interface type and enters its configuration mode. The interface options available are: GE and VLAN                                                                                                                                                                                                               |
| <b>ge 1 &lt;1-48&gt;</b>   | Selects a GE interface to configure <ul style="list-style-type: none"> <li>• 1 - Configures the GE interface unit identifier as 1</li> <li>• &lt;1-48&gt; - Configures the physical port number from 1 - 24/48</li> </ul> <p><b>Note:</b> For the EX3524 model switch the GE port range is 1-24, and for the EX3548 it is 1-48.</p> |
| <b>vlan &lt;1-4094&gt;</b> | Selects a VLAN interface to configure <ul style="list-style-type: none"> <li>• &lt;1-4094&gt; - Specify the VLAN interface ID from 1 - 4094.</li> </ul>                                                                                                                                                                             |

### Example

```

nx4500-5CFA8E(config-profile-testEX35XX)#interface vlan 1
nx4500-5CFA8E(config-profile-testEX35XX-if-vlan1)#?
commands:
 ip Internet Protocol (IP)
 no Negate a command or set its defaults

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx4500-5CFA8E(config-profile-testEX35XX-if-vlan1)#

nx4500-5CFA8E(config-profile-testEX35XX)#interface ge 1 1
nx4500-5CFA8E(config-profile-testEX35XX-if-ge1-1)#?
commands:
 access-group Access group to bind a port to an ACL name
 no Negate a command or set its defaults
 port Configures the characteristics of the port
 power EX3500 Power over Ethernet Command
 shutdown Shutdown the selected interface
 speed-duplex Configures speed and duplex operation
 switchport Configures switch mode characteristics
 use Set setting to use

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx4500-5CFA8E(config-profile-testEX35XX-if-ge1-1)#

```

### Related Commands

|                                                             |                                                                             |
|-------------------------------------------------------------|-----------------------------------------------------------------------------|
| <a href="#">no</a> on page 1314                             | Removes this interface (GE/VLAN) settings from the EX35XX profile or device |
| <a href="#">interface-ge-config commands</a> on page 1299   | Summarizes GE interface configuration mode commands                         |
| <a href="#">interface-vlan-config commands</a> on page 1308 | Summarizes VLAN interface configuration mode commands                       |

## interface-ge-config commands

[interface](#) on page 1297

The following table lists the EX35XX GE interface configuration mode commands:

| Command                                   | Description                                                                                                                          |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">access-group</a> on page 1299 | Binds an EX3500 ACL to the selected port                                                                                             |
| <a href="#">port</a> on page 1300         | Enables port monitoring on the selected port                                                                                         |
| <a href="#">power</a> on page 1302        | Turns power on or off for the selected port                                                                                          |
| <a href="#">shutdown</a> on page 1303     | Shuts down the selected port                                                                                                         |
| <a href="#">speed-duplex</a> on page 1304 | Configures the speed and duplex mode of the selected port when auto-negotiation is disabled. Auto-negotiation is enabled by default. |
| <a href="#">switch-port</a> on page 1304  | Configures the switch mode characteristics of the selected port                                                                      |
| <a href="#">use</a> on page 1306          | Applies a EX3500 QoS policy map with the selected port                                                                               |
| <a href="#">no</a> on page 1307           | Removes or reverts the selected port's settings                                                                                      |

access-group

[interface-ge-config commands](#) on page 1299

Binds an EX3500 ACL to the selected port

When applied to the port, the ACL takes effect. Only one ACL can be bound to a port at a time. In case you bind a new ACL to a port with an existing ACL binding, the old binding is replaced with the new one.

Supported in the following platforms:

- Switches — EX3524, EX3548
- Wireless Controllers — RFS4000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
access-group [ex3500-ext-access-list|ex3500-std-access-list|mac-access-list] <ACL-NAME> in {time-range <TIME-RANGE-NAME>}
```

Parameters

```
access-group [ex3500-ext-access-list|ex3500-std-access-list|mac-access-list] <ACL-NAME> in {time-range <TIME-RANGE-NAME>}
```

|                                                |                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>access-group</b>                            | Binds a EX3500 ACL with this GE port. Select ACL type and specify the ACL name. The ACL should be existing and configured.                                                                                                                                                                                                                 |
| <b>ex3500-ext-access-list &lt;ACL-NAME&gt;</b> | Binds an existing and configured EX3500 extended ACL <ul style="list-style-type: none"> <li>• &lt;ACL-NAME&gt; - Specify the ACL name.</li> </ul>                                                                                                                                                                                          |
| <b>ex3500-std-access-list &lt;ACL-NAME&gt;</b> | Binds an existing and configured EX3500 standard ACL <ul style="list-style-type: none"> <li>• &lt;ACL-NAME&gt; - Specify the ACL name.</li> </ul>                                                                                                                                                                                          |
| <b>mac-access-list &lt;ACL-NAME&gt;</b>        | Binds an existing and configured EX3500 MAC ACL <ul style="list-style-type: none"> <li>• &lt;ACL-NAME&gt; - Specify the MAC ACL name.</li> </ul>                                                                                                                                                                                           |
| <b>in</b>                                      | Applies the specified ACL to all incoming packets                                                                                                                                                                                                                                                                                          |
| <b>time-range &lt;TIME-RANGE-NAME&gt;</b>      | Optional. Associates a EX3500 absolute or periodic time range with this access group. The specified ACL is bound to the port during the time period specified by the associated time range. <ul style="list-style-type: none"> <li>• &lt;TIME-RANGE-NAME&gt; - Specify the time range name (should be existing and configured).</li> </ul> |

#### Example

```
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#access-group ex3500-ext-access-list EX3500_ACL_EXT_1 in time-range EX3500_TimeRange_01
```

```
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#show context
interface ge 1 20
access-group ex3500-ext-access-list EX3500_ACL_EXT_1 in time-range EX3500_TimeRange_01
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#
```

#### Related Commands

|                        |                                        |
|------------------------|----------------------------------------|
| <b>no</b> on page 1307 | Removes the GE port EX3500 ACL binding |
|------------------------|----------------------------------------|

port

[interface-ge-config commands](#) on page 1299

Enables port monitoring on the selected port. This allows the port to monitor specified ports and/or MAC address(es). When enabled, the switch sends a copy of the network packets seen on the specified switch port (or VLAN interface) to the monitoring switch port. These packets are analyzed and debugged to provide vital information, such as network performance, intrusion alerts, etc.

Supported in the following platforms:

- Switches – EX3524, EX3548
- Wireless Controllers – RFS4000
- Service Platforms – NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

#### Syntax

```
port monitor [ethernet | ex3500-ext-access-list | ex3500-std-access-list | mac-access-list | mac-address | vlan]
```

```
port monitor ethernet 1 <1-52> {both/rx/tx}
```



```
port monitor [ex3500-ext-access-list|ex3500-std-access-list|mac-access-list] <ACL-NAME>
```

```
port monitor mac-address <MAC>
```

```
port monitor vlan <1-4094>
```

Parameters

```
port monitor ethernet 1 <1-52> {both|rx|tx}
```

|                                             |                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>port monitor ethernet 1 &lt;1-52&gt;</b> | Configures the characteristics of this GE port <ul style="list-style-type: none"><li>• monitor - Enables monitoring of another port</li><li>• ethernet 1 - Selects Ethernet interface and configures the port identifier as 1</li><li>• &lt;1-52&gt; - Configures the Ethernet unit number from 1 - 52</li></ul> |
| <b>{both rx tx}</b>                         | After specifying the port, optionally configure the following: <ul style="list-style-type: none"><li>• both - Optional. Monitors both incoming and outgoing traffic</li><li>• rx - Optional. Monitors only incoming traffic</li><li>• tx - Optional. Monitors only outgoing traffic</li></ul>                    |

```
port monitor [ex3500-ext-access-list|ex3500-std-access-list|mac-access-list] <ACL-NAME>
```

|                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>port monitor</b>                                                                     | Configures the characteristics of this GE port <ul style="list-style-type: none"><li>• monitor - Enables monitoring of another port</li></ul>                                                                                                                                                                                                                                                                                                      |
| <b>[ex3500-ext-access-list ex3500-std-access-list mac-access-list] &lt;ACL-NAME&gt;</b> | After specifying the port, apply one of the following ACLs: <ul style="list-style-type: none"><li>• ex3500-ext-access-list - Applies a EX3500 extended ACL</li><li>• ex3500-std-access-list - Applies a EX3500 standard ACL</li><li>• mac-access-list - Applies a MAC ACL with EX3500 deny or permit rules<ul style="list-style-type: none"><li>• &lt;ACL-NAME&gt; - Specify the ACL name (should be existing and configured).</li></ul></li></ul> |

```
port monitor mac-address <MAC>
```

|                                |                                                                                                                                                                |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>port monitor</b>            | Configures the characteristics of this GE port <ul style="list-style-type: none"><li>• monitor - Enables monitoring of another port</li></ul>                  |
| <b>mac-address &lt;MAC&gt;</b> | Configures the MAC address to monitor <ul style="list-style-type: none"><li>• &lt;MAC&gt; - Specify the MAC address in the AA-BB-CC-DD-EE-FF format.</li></ul> |

```
port monitor vlan <1-4094>
```

|                            |                                                                                                                                                |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>port monitor</b>        | Configures the characteristics of this GE port <ul style="list-style-type: none"><li>• monitor - Enables monitoring of another port</li></ul>  |
| <b>vlan &lt;1-4094&gt;</b> | Configures the VLAN interface to monitor <ul style="list-style-type: none"><li>• &lt;1-4094&gt; - Specify the VLAN ID from 1 - 4094.</li></ul> |

Example

```
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#port monitor vlan 20
```

```
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#show context
```

```

interface ge 1 20
 access-group ex3500-ext-access-list EX3500_ACL_EXT_1 in time-range EX3500_TimeRange_01
 port monitor vlan 20
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#

```

#### Related Commands

|                                 |                                                                        |
|---------------------------------|------------------------------------------------------------------------|
| <a href="#">no</a> on page 1307 | Disables port monitoring on the selected port and removes the settings |
|---------------------------------|------------------------------------------------------------------------|

#### power

[interface-ge-config commands](#) on page 1299

Enables power allocation to the selected port. When enabled, the power is allocated to this port. Use the command to configure the power allocation settings, such as maximum power allocated, priority level of this port in connection with power allocation, and the time range within which these power settings are applied.

This option is enabled by default.

Supported in the following platforms:

- Switches — EX3524, EX3548
- Wireless Controllers — RFS4000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

#### Syntax

```
power inline {maximum/priority/time-range}
```

```
power inline {maximum allocation milliwatts <3000-34200>}
```

```
power inline {priority [critical/high/low]}
```

```
power inline {time-range <TIME-RANGE-NAME>}
```

#### Parameters

```
power inline {maximum allocation milliwatts <3000-34200>}
```

|                                                         |                                                                                                                                                                                                                                         |
|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>power inline</b>                                     | Turns power on or off for the selected port. This option is enabled by default.                                                                                                                                                         |
| <b>maximum allocation milliwatts &lt;3000-34200&gt;</b> | Optional. Configures the maximum power allocation, in milliwatts, for this port <ul style="list-style-type: none"> <li>• &lt;3000-34200&gt; - Specify a value from 3000 - 34200 milliwatts. The default is 34200 milliwatts.</li> </ul> |

```
power inline {priority [critical/high/low]}
```

|                                     |                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>power inline</b>                 | Turns power on or off for the selected port. This option is enabled by default.                                                                                                                                                                                                                                  |
| <b>priority [critical/high/low]</b> | Optional. Configures the PoE power priority as: <ul style="list-style-type: none"> <li>• critical - Configures the PoE power priority as critical</li> <li>• high - Configures the PoE power priority as high</li> <li>• low - Configures the PoE power priority as low (this is the default setting)</li> </ul> |

```
power inline {time-range <TIME-RANGE-NAME>}
```

|                                                     |                                                                                                                                                                                                 |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>power inline</b>                                 | Turns power on or off for the selected port. This option is enabled by default.                                                                                                                 |
| <b>time-range</b><br><b>&lt;TIME-RANGE-NAME&gt;</b> | Optional. Binds a EX3500 time range to this port <ul style="list-style-type: none"> <li>• &lt;TIME-RANGE-NAME&gt; - Specify the time range name (should be existing and configured).</li> </ul> |

#### Example

```

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#power inline maximum allocation
milliwatts 30000

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#power inline priority critical

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#power inline time-range
EX3500_TimeRange_01

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#show context
interface ge 1 20
power inline maximum allocation milliwatts 30000
power inline priority critical
power inline time-range EX3500_TimeRange_01
access-group ex3500-ext-access-list EX3500_ACL_EXT_1 in time-range EX3500_TimeRange_01
port monitor vlan 20
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#

```

#### Related Commands

|                        |                                                |
|------------------------|------------------------------------------------|
| <b>no</b> on page 1307 | Disables power allocation to the selected port |
|------------------------|------------------------------------------------|

#### shutdown

[interface-ge-config commands](#) on page 1299

Shuts down the selected port

Supported in the following platforms:

- Switches — EX3524, EX3548
- Wireless Controllers — RFS4000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

#### Syntax

**shutdown**

#### Parameters

None

#### Example

```

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#shutdown

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#show context
interface ge 1 20
shutdown
power inline maximum allocation milliwatts 30000
power inline priority critical
power inline time-range EX3500_TimeRange_01
access-group ex3500-ext-access-list EX3500_ACL_EXT_1 in time-range EX3500_TimeRange_01
port monitor vlan 20
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#

```

## Related Commands

|                                 |                           |
|---------------------------------|---------------------------|
| <a href="#">no</a> on page 1307 | Brings up a shutdown port |
|---------------------------------|---------------------------|

## speed-duplex

[interface-ge-config commands](#) on page 1299

Configures the speed and duplex mode of the selected port when auto-negotiation is disabled. Auto-negotiation is enabled by default.

This option is disabled by default.

Supported in the following platforms:

- Switches — EX3524, EX3548
- Wireless Controllers — RFS4000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

## Syntax

```
speed-duplex [100full | 100half | 10full | 10half]
```

## Parameters

```
speed-duplex [100full | 100half | 10full | 10half]
```

|                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>speed-duplex</b><br><b>[100full  </b><br><b>100half  </b><br><b>10full   10half]</b> | Configures the speed and duplex mode of the selected port to one of the following modes: <ul style="list-style-type: none"><li>• 100full – Forces 100 Mbps full-duplex operation</li><li>• 100half – Forces 100 Mbps half-duplex operation</li><li>• 10full – Force 10 Mbps full-duplex operation</li><li>• 10half – Force 10 Mbps half-duplex operation</li></ul> When configured, forces the switch to operate at the specified speed and mode. |
|-----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Example

```
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#speed-duplex 100half

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#show context
interface ge 1 20
 shutdown
 speed-duplex 100half
 power inline maximum allocation milliwatts 30000
 power inline priority critical
 power inline time-range EX3500_TimeRange_01
 access-group ex3500-ext-access-list EX3500_ACL_EXT_1 in time-range EX3500_TimeRange_01
 port monitor vlan 20
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#
```

## Related Commands

|                                 |                                                                          |
|---------------------------------|--------------------------------------------------------------------------|
| <a href="#">no</a> on page 1307 | Removes the speed and duplex settings configured for this EX35XX profile |
|---------------------------------|--------------------------------------------------------------------------|

## switch-port

[interface-ge-config commands](#) on page 1299

Configures the switch mode characteristics of the selected port

Supported in the following platforms:

- Switches – EX3524, EX3548
- Wireless Controllers – RFS4000
- Service Platforms – NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
switchport [allowed|l2protocol-tunnel|mode|native]
```

```
switchport allowed [add <VLAN-ID>|none|remove <VLAN-ID>]
```

```
switchport l2protocol-tunnel [cdp|lldp|pvst+|spanning-tree|vtp]
```

```
switchport mode [access|hybrid|trunk]
```

```
switchport native
```

Parameters

```
switchport allowed [add <VLAN-ID>|none|remove <VLAN-ID>]
```

|                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>switchport allowed [add &lt;VLAN-ID&gt;   none   remove &lt;VLAN-ID&gt;]</b> | <p>Configures VLAN groups on the selected interface.</p> <ul style="list-style-type: none"><li>• add &lt;VLAN-ID&gt; - Configures the list of VLAN identifiers to add. When the add option is used, the interface is assigned to the specified VLANs, and membership in all previous VLANs is retained.</li><li>• &lt;VLAN-ID&gt; - Specify the list of VLANs to add.</li><li>• none - Removes all VLANs from the current list</li><li>• remove &lt;VLAN-ID&gt; - Configures the list of VLAN identifiers to remove. When the remove option is used, the specified VLANs are removed from the current list.</li><li>• &lt;VLAN-ID&gt; - Specify the list of VLANs to remove.</li></ul> |
|---------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
switchport l2protocol-tunnel [cdp|lldp|pvst+|spanning-tree|vtp]
```

|                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>switchport l2protocol-tunnel [cdp lldp pvst+ spanning-tree vtp]</b> | <p>Enables layer 2 protocol tunneling (L2PT) for the specified protocol. Specify the protocol:</p> <ul style="list-style-type: none"><li>• cdp - Cisco Discovery Protocol</li><li>• lldp - Link Layer Discovery Protocol</li><li>• pvst+ - Cisco Per VLAN Spanning Tree Plus</li><li>• spanning-tree - Spanning Tree (STP, RSTP, MSTP)</li><li>• vtp - Cisco VLAN Trunking Protocol</li></ul> <p>L2PT is disabled for all of the above specified protocols by default.</p> |
|------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
switchport mode [access|hybrid|trunk]
```

|                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>switchport mode [access hybrid trunk]</b> | <p>Configures the VLAN membership mode for this port</p> <ul style="list-style-type: none"> <li>• access – The port is configured as an access VLAN interface. It transmits and receives packets untagged frames on a single VLAN.</li> <li>• trunk – Configures the selected port as an end-point for a VLAN trunk. A trunk link is configured between two switches, and it carries frames on more than one VLANs. These frames are tagged in order to identify the source VLAN. Frames belonging to the port's default VLAN are also transmitted as tagged frames.</li> <li>• hybrid – Configures the selected port as a hybrid VLAN interface. When configured as hybrid, the port can transmit either tagged or untagged frames. This is the default setting.</li> </ul> |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
switchport native vlan <1-4094>
```

|                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>switchport native vlan &lt;1-4094&gt; in</b> | <p>Configures the VLAN membership mode for this port</p> <ul style="list-style-type: none"> <li>• native vlan &lt;1-4094&gt; – Configures the port's VLAN ID (PVID) (this is the port's default VLAN ID). Frames from the specified VLAN ingress untagged at this port. The default value is 1.</li> </ul> <p>When using access mode, and an interface is assigned to a new VLAN, the port's VLAN ID (PVID) is automatically set to the identifier for that VLAN. When using hybrid mode, the PVID for an interface can be set to any VLAN for which it is an untagged member.</p> |
|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Example

```
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#switchport mode access
```

```
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#show context
interface ge 1 20
 shutdown
 speed-duplex 100half
 switchport mode access
 power inline maximum allocation milliwatts 30000
 power inline priority critical
 power inline time-range EX3500_TimeRange_01
 access-group ex3500-ext-access-list EX3500_ACL_EXT_1 in time-range EX3500_TimeRange_01
 port monitor vlan 20
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#
```

#### Related Commands

|                                 |                                                        |
|---------------------------------|--------------------------------------------------------|
| <a href="#">no</a> on page 1307 | Removes the selected port's switchport characteristics |
|---------------------------------|--------------------------------------------------------|

use

[interface-ge-config commands](#) on page 1299

Applies a EX3500 QoS policy map with the selected port

Supported in the following platforms:

- Switches – EX3524, EX3548
- Wireless Controllers – RFS4000
- Service Platforms – NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

#### Syntax

```
use ex3500-policy-map <EX3500-QoS-POLICY-MAP-NAME> in
```

## Parameters

`use ex3500-policy-map <EX3500-QoS-POLICY-MAP-NAME> in`

|                                                                 |                                                                                                             |
|-----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| <b>use ex3500-policy-map &lt;EX3500-QoS-POLICY-MAP-NAME&gt;</b> | Applies a EX3500 QoS policy map with the selected port                                                      |
|                                                                 | • <EX3500-QoS-POLICY-MAP-NAME> - Specify the EX3500 QoS policy map name (should be existing and configured) |
|                                                                 | • in - Applies the specified policy to traffic ingressing at the selected port.                             |

## Example

```
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#use ex3500-policy-map in test

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#show context
interface ge 1 20
 shutdown
 speed-duplex 100half
 switchport mode access
 use ex3500-policy-map in test
 power inline maximum allocation milliwatts 30000
 power inline priority critical
 power inline time-range EX3500_TimeRange_01
 access-group ex3500-ext-access-list EX3500_ACL_EXT_1 in time-range EX3500_TimeRange_01
 port monitor vlan 20
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#
```

## Related Commands

|                                 |                                                                       |
|---------------------------------|-----------------------------------------------------------------------|
| <a href="#">no</a> on page 1307 | Disassociates the EX3500 QoS policy map linked to this EX3500 profile |
|---------------------------------|-----------------------------------------------------------------------|

`no`

[interface-ge-config commands](#) on page 1299

Removes or reverts the selected port's settings

Supported in the following platforms:

- Switches – EX3524, EX3548

### Syntax

```
no [access-group | port | power | shutdown | speed-duplex | switchport | use]
```

```
no access-group [ex3500-ext-access-list | ex3500-std-access-list | mac-access-list] <ACL-NAME> in
```

```
no port monitor [ethernet | ex3500-ext-access-list | ex3500-std-access-list | mac-access-list | mac-address | vlan]
```

```
no port monitor ethernet 1 <1-52>
```

```
no port monitor [ex3500-ext-access-list | ex3500-std-access-list | mac-access-list] <ACL-NAME>
```

```
no port monitor mac-address <MAC>
```

```
no port monitor vlan <1-4094>
```

```

no power inline {maximum allocation/priority/time-range}

no shutdown

no speed-duplex

no switchport [l2protocol-tunnel [cdp|lldp|pvst+|spanning-tree|vtp]|
native vlan]

no use ex3500-policy-map in

```

Parameters  
no <PARAMETERS>

|                           |                                                                                |
|---------------------------|--------------------------------------------------------------------------------|
| <b>no</b>                 | Removes or reverts the selected port's settings based on the parameters passed |
| <b>&lt;PARAMETERS&gt;</b> |                                                                                |

### Example

The following example shows the EX3524 profile's GE port 20's settings before the 'no' commands are executed:

```

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#show context
interface ge 1 20
 shutdown
 speed-duplex 100half
 switchport mode access
 use ex3500-policy-map in test
 power inline maximum allocation milliwatts 30000
 power inline priority critical
 power inline time-range EX3500_TimeRange_01
 access-group ex3500-ext-access-list EX3500_ACL_EXT_1 in time-range EX3500_TimeRange_01
 port monitor vlan 20
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#

```

```

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#no shutdown
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#no power inline maximum allocation
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#no use ex3500-policy-map in

```

The following example shows the EX3524 profile's GE port 20's settings after the 'no' commands are executed:

```

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#show context
interface ge 1 20
 speed-duplex 100half
 switchport mode access
 power inline maximum allocation milliwatts 32400
 power inline priority critical
 power inline time-range EX3500_TimeRange_01
 access-group ex3500-ext-access-list EX3500_ACL_EXT_1 in time-range EX3500_TimeRange_01
 port monitor vlan 20
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#

```

## Interface-vlan-config commands

[interface](#) on page 1297

The following table lists the VLAN interface configuration mode commands:



| Command                      | Description                                                        |
|------------------------------|--------------------------------------------------------------------|
| <code>ip</code> on page 1309 | Configures IP related settings for this VLAN interface             |
| <code>no</code> on page 1310 | Removes the IP related settings configured for this VLAN interface |

ip

[interface-vlan-config commands](#) on page 1308

Configures IP related settings for this VLAN interface

Supported in the following platforms:

- Switches – EX3524, EX3548
- Wireless Controllers – RFS4000
- Service Platforms – NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
ip address [<IP/M>|bootp|dhcp]
```

```
ip address <IP/M> {default-gateway <IP>|secondary <IP>}
```

```
ip address [bootp|dhcp]
```

Parameters

```
ip address <IP/M> {default-gateway <IP>|secondary <IP>}
```

|                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre><b>ip address</b><br/><b>&lt;IP/M&gt;</b><br/><b>{default-</b><br/><b>gateway &lt;IP&gt; </b><br/><b>secondary</b><br/><b>&lt;IP&gt;}</b></pre> | <p>Manually configures the selected VLAN interface's primary and secondary IPv4 addresses. It also allows to optionally configure the default gateway.</p> <ul style="list-style-type: none"> <li>• <code>&lt;IP/M&gt;</code> – Manually configures this VLAN interface's IP address in the A.B.C.D/M format. Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets. The network mask can be either in the traditional format xxx.xxx.xxx.xxx or use classless format with the range /5 to /32. For example the subnet 255.255.224.0 would be /19.</li> <li>• <code>default-gateway &lt;IP&gt;</code> – Optional. Configures the default gateway's IP address. This is the gateway through which this switch can reach other subnets not found in the local routing table. Before specifying the default gateway, ensure that the network interface directly connecting to the gateway is configured on the route. By default no gateway is specified. <ul style="list-style-type: none"> <li><code>&lt;IP&gt;</code> – Specify the IP address in the A.B.C.D address.</li> </ul> </li> <li>• <code>secondary &lt;IP&gt;</code> – Optional. Configures this VLAN interface's secondary IP address <ul style="list-style-type: none"> <li><code>&lt;IP&gt;</code> – Specify the secondary IP address in the A.B.C.D address</li> </ul> </li> </ul> |
|------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
ip address [bootp|dhcp]
```

|                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre><b>ip address</b><br/><b>[bootp dhcp]</b></pre> | <p>Enables a DHCP or Bootp server to provide the primary IPv4 address for the selected VLAN interface</p> <ul style="list-style-type: none"> <li>• <code>bootp</code> – Enables the VLAN interface to get its IP address from a Bootp server</li> <li>• <code>dhcp</code> – Enables the VLAN interface to get its IP address from a DHCP server</li> </ul> <p>If selecting DHCP/Bootp, ensure that a server on the network has been configured to provide the necessary configuration to the switch. Using DHCP or Bootp results in frequent connectivity loss between the browser interface and the switch. Further, DHCP and Bootp cannot configure secondary IP addresses needed for multinetting.</p> |
|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Example

```
nx9500-6C8809(config-profile-testEX3524-if-vlan20)#ip address 192.168.13.28/24 default-gateway 192.168.13.13
```

```
nx9500-6C8809(config-profile-testEX3524-if-vlan20)#show context
interface vlan 20
 ip address 192.168.13.28/24 default-gateway 192.168.13.13
nx9500-6C8809(config-profile-testEX3524-if-vlan20)#
```

## Related Commands

|                              |                                                           |
|------------------------------|-----------------------------------------------------------|
| <code>no</code> on page 1310 | Removes the IP address configured for this VLAN interface |
|------------------------------|-----------------------------------------------------------|

`no`

[interface-vlan-config commands](#) on page 1308

Removes the IP related settings configured for this VLAN interface

Supported in the following platforms:

- Switches – EX3524, EX3548
- Wireless Controllers – RFS4000
- Service Platforms – NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

## Syntax

```
no ip address [<IP/M> | bootp | dhcp]
```

## Parameters

```
no <PARAMETERS>
```

|                                                    |                                                                               |
|----------------------------------------------------|-------------------------------------------------------------------------------|
| <code>no</code><br><code>&lt;PARAMETERS&gt;</code> | Removes this EX3500's selected VLAN's settings based on the parameters passed |
|----------------------------------------------------|-------------------------------------------------------------------------------|

## Example

The following example shows the interface VLAN 20 setting before the 'no' command is executed:

```
nx9500-6C8809(config-profile-testEX3524-if-vlan20)#show context
interface vlan 20
 ip address 192.168.13.28/24 default-gateway 192.168.13.13
nx9500-6C8809(config-profile-testEX3524-if-vlan20)#
```

```
nx9500-6C8809(config-profile-testEX3524-if-vlan20)#no ip address 192.168.13.28/24
```

The following example shows the interface VLAN 20 setting after the 'no' command is executed:

```
nx9500-6C8809(config-profile-testEX3524-if-vlan20)#show context
interface vlan 20
nx9500-6C8809(config-profile-testEX3524-if-vlan20)#
```

`ip`

[EX3524 & EX3548 Profile/Device Config Commands](#) on page 1296

Configures the default gateway through which this EX35XX switch can reach other subnets

## Supported in the following platforms:

- Switches – EX3524, EX3548

- Wireless Controllers – RFS4000
- Service Platforms – NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

### Syntax

```
ip default-gateway <IP>
```

### Parameters

```
ip default-gateway <IP>
```

|                                      |                                                                   |
|--------------------------------------|-------------------------------------------------------------------|
| <b>ip default-gateway &lt;IP&gt;</b> | Configures the default gateway's IP address in the A.B.C.D format |
|                                      | • <IP> – Specify the IP address.                                  |

### Example

```
nx9500-6C8809(config-profile-testEX3524)#ip default-gateway 192.168.13.13
```

```
nx9500-6C8809(config-profile-testEX3524)#show context
```

```
profile ex3524 testEX3524
 ip default-gateway 192.168.13.13
 no autoinstall configuration
 no autoinstall firmware
 interface ge 1 17
 interface ge 1 16
 interface ge 1 15
 interface ge 1 14
 interface ge 1 13
 interface ge 1 12
 interface ge 1 11
```

```
--More--
```

```
 interface ge 1 21
 use firewall-policy default
 service pm sys-restart
 nx9500-6C8809(config-profile-testEX3524)#
```

*power*

[EX3524 & EX3548 Profile/Device Config Commands](#) on page 1296

Enables power inline compatibility mode on this EX35XX profile. This option is disabled by default.

### Supported in the following platforms:

- Switches – EX3524, EX3548
- Wireless Controllers – RFS4000
- Service Platforms – NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

### Syntax

```
power inline compatible
```

### Parameters

```
power inline compatible
```

|                                |                                         |
|--------------------------------|-----------------------------------------|
| <b>power inline compatible</b> | Enables power inline compatibility mode |
|--------------------------------|-----------------------------------------|

## Example

```
nx9500-6C8809(config-profile-testEX3524)#power inline compatible

nx9500-6C8809(config-profile-testEX3524)#show context
profile ex3524 testEX3524
 ip default-gateway 192.168.13.13
 power inline compatible
 no autoinstall configuration
 no autoinstall firmware
 interface ge 1 17
 interface ge 1 16
 interface ge 1 15
 interface ge 1 14
 interface ge 1 13
 interface ge 1 12
 --More--
nx9500-6C8809(config-profile-testEX3524)#
```

## upgrade

[EX3524 & EX3548 Profile/Device Config Commands](#) on page 1296

Configures adopted EX35XX switch upgrade settings

For a EX35XX switch to adopt to and be managed by a WiNG controller, you need to upload two images on the switch. An operation code (opcode) image and an adopted image. The opcode image functions as an operating system that enables the WiNG controller to communicate with the EX35XX switch. This command allows you to configure the EX35XX's opcode image upgrade settings.

### Supported in the following platforms:

- Switches — EX3524, EX3548
- Wireless Controllers — RFS4000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

### Syntax

```
upgrade opcode [auto|path <LINE>|reload]
```

### Parameters

```
upgrade opcode [auto|path <LINE>|reload]
```

|                          |                                                                       |
|--------------------------|-----------------------------------------------------------------------|
| <b>upgrade opcode</b>    | Configures the opcode image upgrade settings                          |
| <b>auto</b>              | Enables automatic upgrade                                             |
| <b>path &lt;LINE&gt;</b> | Configures the location of the opcode image                           |
| <b>reload</b>            | Enables automatic reload after successful loading of the opcode image |

### Example

```
<EX35XX-DEVICE>#show versions
Unit 1
Serial Number : 14136520900352
Hardware Version : R01
EPLD Version : 0.00
Number of Ports : 28
Main Power Status : Up
```

```

Role : Master
Loader Version : 5.0.0.1-01A
Linux Kernel Version : 2.6.22.18
Boot ROM Version : 0.0.0.1
Operation Code Version : 5.0.0.0-03D
Adoptd Version : 5.8.3.0-024D
<EX35XX-DEVICE>#

nx9500-6C8809(config-profile-testEX3524)#upgrade auto
nx9500-6C8809(config-profile-testEX3524)#upgrade reload
nx9500-6C8809(config-profile-testEX3524)#upgrade opcode path ftp://
anonymous:anonymous@192.168.13.10/ex35xx/EX3524.img

nx9500-6C8809(config-profile-testEX3524)#show context
profile ex3524 testEX3524
 ip default-gateway 192.168.13.13
 power inline compatible
.....
 use firewall-policy default
 service pm sys-restart
 upgrade opcode auto
 upgrade opcode path ftp://anonymous:anonymous@192.168.13.10/ex35xx/EX3524.img
 upgrade opcode reload
nx9500-6C8809(config-profile-testEX3524)#

```

#### use

[EX3524 & EX3548 Profile/Device Config Commands](#) on page 1296

Applies an EX3500 management policy to this EX35XX profile

#### Supported in the following platforms:

- Switches — EX3524, EX3548
- Wireless Controllers — RFS4000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

#### Syntax

```
use ex3500-management-policy <POLICY-NAME>
```

#### Parameters

```
use ex3500-management-policy <POLICY-NAME>
```

|                                                         |                                                                                                                                                                                                                            |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>use ex3500-management-policy &lt;POLICY-NAME&gt;</b> | <p>Applies an EX3500 management policy to this EX35XX profile</p> <ul style="list-style-type: none"> <li>• &lt;POLICY-NAME&gt; - Specify the EX3500 management policy name (should be existing and configured).</li> </ul> |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Example

```

nx9500-6C8809(config-profile-testEX3524)#use ex3500-management-policy test
Trustpoints HTTPS Server and RSA keys for SSH can be configured with 'trustpoint' and 'rsa-key' commands in device context
nx9500-6C8809(config-profile-testEX3524)#

nx9500-6C8809(config-profile-testEX3524)#show context
profile ex3524 testEX3524
 ip default-gateway 192.168.13.13
 power inline compatible

```

```

no autoinstall configuration
no autoinstall firmware
interface ge 1 17
interface ge 1 16
interface ge 1 15
--More--
use ex3500-management-policy test
use firewall-policy default
service pm sys-restart
upgrade opcode auto
upgrade opcode path ftp://anonymous:anonymous@192.168.13.10/ex35xx/EX3524.img
upgrade opcode reload
nx9500-6C8809(config-profile-testEX3524)#

```

no

[EX3524 & EX3548 Profile/Device Config Commands](#) on page 1296

Removes or reverts this EX3500 profile's settings

#### Supported in the following platforms:

- Switches – EX3524, EX3548
- Wireless Controllers – RFS4000
- Service Platforms – NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

#### Syntax

```

no [interface vlan <1-4094>|default-gateway {<IP>}|power inline
compatible| upgrade opcode [auto|path|reload]|use ex3500-management-
policy]

```

#### Parameters

no <PARAMETERS>

|                           |                                                                                |
|---------------------------|--------------------------------------------------------------------------------|
| <b>no</b>                 | Removes or reverts this EX3500 profile settings based on the parameters passed |
| <b>&lt;PARAMETERS&gt;</b> |                                                                                |

#### Example

```

nx9500-6C8809(config-profile-testEX3524)#show context
profile ex3524 testEX3524
ip default-gateway 192.168.13.13
power inline compatible
no autoinstall configuration
no autoinstall firmware
interface ge 1 17
interface ge 1 16
interface ge 1 15
interface ge 1 14
interface ge 1 13
interface ge 1 12
interface ge 1 11
interface ge 1 10
interface ge 1 24
interface ge 1 22
interface vlan 20
interface ge 1 23
--More--
use ex3500-management-policy test

```

```
use firewall-policy default
service pm sys-restart
upgrade opcode auto
upgrade opcode path ftp://anonymous:anonymous@192.168.13.10/ex35xx/EX3524.img
upgrade opcode reload
nx9500-6C8809(config-profile-testEX3524)#

nx9500-6C8809(config-profile-testEX3524)#no use ex3500-management-policy
nx9500-6C8809(config-profile-testEX3524)#no upgrade opcode reload
nx9500-6C8809(config-profile-testEX3524)#no interface vlan 20

nx9500-6C8809(config-profile-testEX3524)#show context
profile ex3524 testEX3524
ip default-gateway 192.168.13.13
power inline compatible
no autoinstall configuration
--More--
use firewall-policy default
service pm sys-restart
upgrade opcode auto
upgrade opcode path ftp://anonymous:anonymous@192.168.13.10/ex35xx/EX3524.img
nx9500-6C8809(config-profile-testEX3524)#
```

# AAA POLICY COMMANDS

## AAA-POLICY

---

This chapter summarizes the AAA (Authentication, Authorization, and Accounting) policy commands in the CLI command structure.

A AAA policy enables administrators to define access control settings governing network permissions. External RADIUS and LDAP servers (AAA servers) also provide user database information and user authentication data. Each WLAN maintains its own unique AAA configuration.

AAA provides a modular way of performing the following services:

**Authentication** — Provides a means for identifying users, including login and password dialog, challenge and response, messaging support and (depending on the security protocol), encryption. Authentication is the technique by which a user is identified before allowed access to the network. Configure AAA authentication by defining a list of authentication methods, and then applying the list to various interfaces. The list defines the authentication schemes performed and their sequence. The list must be applied to an interface before the defined authentication technique is conducted.

**Authorization** — Authorization occurs immediately after authentication. Authorization is a method for remote access control, including authorization for services and individual user accounts and profiles. Authorization functions through the assembly of attribute sets describing what the user is authorized to perform. These attributes are compared to information contained in a database for a given user and the result is returned to AAA to determine the user's actual capabilities and restrictions. The database could be located locally or be hosted remotely on a RADIUS server. Remote RADIUS servers authorize users by associating AV (attribute-value) pairs with the appropriate user. Each authorization method must be defined through AAA. When AAA authorization is enabled it's applied equally to all interfaces.

**Accounting** — Collects and sends security server information for billing, auditing, and reporting user data; such as start and stop times, executed commands (such as PPP), number of packets, and number of bytes. Accounting enables wireless network administrators to track the services users are accessing and the network resources they are consuming. When accounting is enabled, the network access server reports user activity to a RADIUS security server in the form of accounting records. Each accounting record is comprised of AV pairs and is stored locally on the access control server. The data can be analyzed for network management, client billing, and/or auditing. Accounting methods must be defined through AAA. When AAA accounting is activated, it is applied equally to all interfaces on the access servers.

Use the (config) instance to configure AAA policy commands. To navigate to the config-aaa-policy instance, use the following commands:

```
nx9500-6C8809(config)#aaa-policy test
nx9500-6C8809(config-aaa-policy-test)#?
AAA Policy Mode commands:
 accounting Configure accounting parameters
 attribute Configure RADIUS attributes in access and accounting
 requests
 authentication Configure authentication parameters
 health-check Configure server health-check parameters
```



```

mac-address-format Configure the format in which the MAC address must be
 filled in the Radius-Request frames
no
proxy-attribute Configure radius attribute behavior when proxying
 through controller or rf-domain-manager
server-pooling-mode Configure the method of selecting a server from the
 pool of configured AAA servers
use Set setting to use

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
--More--
nx9500-6C8809(config-aaa-policy-test)#

```

## aaa-policy-commands

The following table summarizes the AAA policy configuration mode commands:

**Table 35: AAA Policy Configuration Commands**

| Command                                          | Description                                                                                                              |
|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <a href="#">accounting</a> on page 1318          | Configures accounting parameters                                                                                         |
| <a href="#">attribute</a> on page 1321           | Configure RADIUS attributes in access and accounting requests                                                            |
| <a href="#">authentication</a> on page 1324      | Configures authentication parameters                                                                                     |
| <a href="#">health-check</a> on page 1329        | Configures health check parameters                                                                                       |
| <a href="#">mac-address-format</a> on page 1330  | Configures the MAC address format                                                                                        |
| <a href="#">proxy-attribute</a> on page 1331     | Configures the RADIUS server's attribute behavior when proxying through the wireless controller or the RF Domain manager |
| <a href="#">server-pooling-mode</a> on page 1332 | Defines the method for selecting a server from the pool of configured AAA servers                                        |
| <a href="#">use</a> on page 1333                 | Defines the AAA command settings                                                                                         |
| <a href="#">no</a> on page 1334                  | Negates a command or sets its default                                                                                    |



### Note

For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see [COMMON COMMANDS](#) on page 640.



### Note

The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (\_) character. In other words, the name of a device cannot contain an underscore.

## accounting

Configures the server type and interval at which interim accounting updates are sent to the server. A maximum of 6 accounting servers can be configured.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
accounting [interim|server|type]
accounting interim interval <60-3600>
accounting server [<1-6>|preference]
accounting server preference [auth-server-host|auth-server-number|none]
accounting server <1-6> [dscp|host|nai-routing|onboard|proxy-mode|retry-timeout-factor|
timeout]
accounting server <1-6> [dscp <0-63>|retry-timeout-factor <50-200>]
accounting server <1-6> host <IP/HOSTNAME/HOST-ALIAS> secret [0 <SECRET>|2 <SECRET>|
<SECRET>]
{port <1-65535>}
accounting server <1-6> nai-routing realm-type [prefix|suffix] realm <REALM-TEXT> {strip}
accounting server <1-6> onboard [centralized-controller|self|controller]
accounting server <1-6> proxy-mode [none|through-centralized-controller|through-controller|
through-mint-host <HOSTNAME/MINT-ID>|through-rf-domain-manager]
accounting server <1-6> timeout <1-60> {attempts <1-10>}
accounting type [start-interim-stop|start-stop|stop-only]
```

### Parameters

```
accounting interim interval <60-3600>
```

|                    |                                                                                                                                           |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| interim            | Configures the interim accounting interval. This is the interval at which interim accounting updates are posted to the accounting server. |
| interval <60-3000> | Specify the interim interval from 60 - 3600 seconds. The default is 1800 seconds.                                                         |

```
accounting server preference [auth-server-host|auth-server-number|none]
```

|                    |                                                                                                                                                                                                                     |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| server             | Configures the RADIUS accounting server's settings                                                                                                                                                                  |
| preference         | Configures the accounting server's preference mode. Authentication requests are forwarded to an accounting server, from the pool, based on the preference mode selected.                                            |
| auth-server-host   | Sets the authentication server as the accounting server. This is the default setting. This parameter indicates the same server is used for authentication and accounting. The server is identified by its hostname. |
| auth-server-number | Sets the authentication server as the accounting server. This parameter indicates the same server is used for authentication and accounting. The server is identified by its index number.                          |
| none               | Indicates the accounting server is independent of the authentication server                                                                                                                                         |

```
accounting server <1-6> [dscp <0-63>|retry-timeout-factor <50-200>]
```

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| server <1-6>                  | Configures an accounting server. Up to 6 accounting servers can be configured.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| dscp <0-63>                   | Sets the DSCP (Differentiated Services Code Point) value for QoS (Quality of Service) monitoring. This value is used in generated RADIUS packets. <ul style="list-style-type: none"> <li>• &lt;0-63&gt; - Sets the DSCP value from 0 - 63. The default value is 34.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                         |
| retry-timeout-factor <50-200> | Sets the scaling factor for retransmission timeouts. The timeout at each attempt is a function of this retry-timeout factor and the attempt number. <ul style="list-style-type: none"> <li>• &lt;50-200&gt; - Specify a value from 50 - 200. The default is 100.</li> </ul> <p>If the scaling factor is 100, the interval between two consecutive retries remains the same, irrespective of the number of retries.</p> <p>If the scaling factor is less than 100, the interval between two consecutive retries reduces with subsequent retries.</p> <p>If this scaling factor is greater than 100, the interval between two consecutive retries increases with subsequent retries.</p> |

```
accounting server <1-6> host <IP/HOSTNAME/HOST-ALIAS> secret [0 <SECRET>|2 <SECRET>|<SECRET>] {port <1-65535>}
```

|                                         |                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| server <1-6>                            | Configures an accounting server. Up to 6 accounting servers can be configured.                                                                                                                                                                                                                                                                                     |
| host <IP/HOSTNAME/HOST-ALIAS>           | Configures the accounting server's hostname IP address, or host-alias<br>The host alias should be existing and configured.                                                                                                                                                                                                                                         |
| secret [0 <SECRET> 2 <SECRET> <SECRET>] | Configures a common secret key used to authenticate with the accounting server <ul style="list-style-type: none"> <li>• 0 &lt;SECRET&gt; - Configures a clear text secret key</li> <li>• 2 &lt;SECRET&gt; - Configures an encrypted secret key</li> <li>• &lt;SECRET&gt; - Specify the secret key. This shared secret should not exceed 127 characters.</li> </ul> |
| port <1-65535>                          | Optional. Configures the accounting server's UDP port (the port used to connect to the accounting server) <ul style="list-style-type: none"> <li>• &lt;1-65535&gt; - Specify the port number from 1 - 65535. The default value is 1813.</li> </ul>                                                                                                                 |

```
accounting server <1-6> nai-routing realm-type [prefix|suffix] realm <REALM-TEXT> {strip}
```

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| server <1-6> | Configures an accounting server. Up to 6 accounting servers can be configured.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| nai-routing  | Enables NAI (Network Access Identifier) routing. This option is disabled by default.<br>The NAI is a character string in the format of an e-mail address as either user or user@realm but it need not be a valid e-mail address or a fully qualified domain name. AAA servers identify clients using the NAI. The NAI can be used either in a specific or generic form. The specific form, which must contain the user portion and may contain the @realm portion, identifies a single user. Using the generic form allows all users to be configured on a single command line, irrespective of whether the users are within a realm or not. Each user still needs a unique security association, but these associations can be stored on a AAA server. The original purpose of the NAI was to support roaming between dial up ISPs. With NAI, an ISP does not have the accounts for all of its roaming partners in a single RADIUS database. RADIUS servers can proxy requests to remote servers as need be. |
| realm-type   | Specifies whether the prefix or suffix of the username is used as the match criteria. For example, if the option selected is prefix, the username's prefix is matched to the realm.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [prefix<br>suffix]        | Select one of the following options: <ul style="list-style-type: none"> <li>prefix - Matches the prefix of the username (For example, username is of type DOMAIN/user1, DOMAIN/user2). This is the default setting.</li> <li>suffix - Matches the suffix of the username (For example, user1@DOMAIN, user2)@DOMAIN)</li> </ul>                                                                                                                                              |
| realm<br><REALM-<br>TEXT> | Configures the text matched against the username. Enter the realm name (should not exceed 50 characters). When the RADIUS accounting server receives a request for a user name, the server references a table of user names. If the user name is known, the server proxies the request to the RADIUS server. <ul style="list-style-type: none"> <li>&lt;REALM-TEXT&gt; - Specifies the matching text including the delimiter (a delimiter is typically " or '@')</li> </ul> |
| strip                     | Optional. When enabled, strips the realm from the username before forwarding the request to the RADIUS server. This option is disabled by default.                                                                                                                                                                                                                                                                                                                          |

```
accounting server <1-6> onboard [centralized-controller|self|controller]
```

|                        |                                                                                                                  |
|------------------------|------------------------------------------------------------------------------------------------------------------|
| server <1-6>           | Configures an accounting server. Up to 6 accounting servers can be configured.                                   |
| onboard                | Selects an onboard server instead of an external host                                                            |
| centralized-controller | Configures the server on the centralized controller managing the network                                         |
| self                   | Configures the onboard server on a AP, wireless controller, or service platform (where the client is associated) |
| controller             | Configures local RADIUS server settings                                                                          |

```
accounting server <1-6> proxy-mode [none|through-centralized-controller|
through-controller|through-mint-host <HOSTNAME/MINT-ID>|through-rf-domain-manager]
```

|                                         |                                                                                                                         |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| server <1-6>                            | Configures an accounting server. Up to 6 accounting servers can be configured.                                          |
| proxy-mode                              | Configures the mode used to proxy requests. The options are: none, through-controller, and through-rf-domain-manager.   |
| none                                    | No proxy required. Sends the request directly using the IP address of the device. This is the default setting.          |
| through-centralized-controller          | Proxies requests through the centralized controller that is configuring and managing the network                        |
| through-controller                      | Proxies requests through the controller (access point, wireless controller, or service platform) configuring the device |
| through-mint-host<br><HOSTNAME/MINT-ID> | Proxies requests through a neighboring MiNT device. Provide the device's MiNT ID or hostname.                           |
| through-rf-domain- manager              | Proxies requests through the local RF Domain Manager                                                                    |

```
accounting server <1-6> timeout <1-60> {attempts <1-10>}
```

|                  |                                                                                                                                                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| server <1-6>     | Configures an accounting server. Up to 6 accounting servers can be configured.                                                                                                                                   |
| timeout <1-60>   | Configures the timeout for each request sent to the RADIUS server <ul style="list-style-type: none"> <li>• &lt;1-60&gt; – Specify a value from 1 - 60 seconds. The default is 5 seconds.</li> </ul>              |
| {attempts<1-10>} | Optional. Specifies the number of attempts made at transmitting a request before being dropped <ul style="list-style-type: none"> <li>• &lt;1-10&gt; – Specify a value from 1 - 10. The default is 3.</li> </ul> |

accounting type [start-interim-stop|start-stop|stop-only]

|                    |                                                                                                                                                                     |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| type               | Configures the type of RADIUS accounting packets sent. The options are: start-interim-stop, start-stop, and stop-only.                                              |
| start-interim-stop | Sends accounting-start and accounting-stop messages at the start and end of the session. This option also sends interim accounting updates.                         |
| start-stop         | Sends only accounting-start and accounting-stop messages at the start and end of the session. Interim accounting updates are not sent. This is the default setting. |
| stop-only          | Sends only an accounting-stop message at the end of the session                                                                                                     |

### Examples

```

nx9500-6C8809(config-aaa-policy-test)#accounting interim interval 65
nx9500-6C8809(config-aaa-policy-test)#accounting server 2 host 172.16.10.10 secret
test1 port 1
nx9500-6C8809(config-aaa-policy-test)#accounting server 2 timeout 2 attempts 2
nx9500-6C8809(config-aaa-policy-test)#accounting type start-stop
nx9500-6C8809(config-aaa-policy-test)#accounting server preference auth-server-number
nx9500-6C8809(config-aaa-policy-test)#show context
aaa-policy test
 accounting server 2 host 172.16.10.10 secret 0 test1 port 1
 accounting server 2 timeout 2 attempts 2
 accounting interim interval 65
 accounting server preference auth-server-number
nx9500-6C8809(config-aaa-policy-test)#

```

### Related Commands

|    |                                                |
|----|------------------------------------------------|
| no | Removes or resets accounting server parameters |
|----|------------------------------------------------|

### attribute

Configures RADIUS Framed-MTU attribute used in access and accounting requests. The Framed-MTU attribute reduces the EAP (Extensible Authentication Protocol) packet size of the RADIUS server. This command is useful in networks where routers and firewalls do not perform fragmentation.

To ensure network security, some firewall software drop UDP fragments from RADIUS server EAP packets. Consequently, the packets are large. Using Framed MTU (Maximum Transmission Unit) reduces the packet size. EAP authentication uses Framed MTU to notify the RADIUS server about the MTU negotiation with the client. The RADIUS server communications with the client do not include EAP messages that cannot be delivered over the network.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533

- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
attribute [acct-delay-time|acct-multi-session-id|chargeable-user-identity|
cisco-vsa|framed-ip-address|framed-mtu|location-information|nas-ip-address|nas-ipv6-
address|
operator-name|service-type]
attribute acct-delay-time
attribute acct-multi-session-id
attribute chargeable-user-identity
attribute cisco-vsa audit-session-id
attribute framed-ip-address
attribute framed-mtu <100-1500>
attribute location-information [include-always|none|server-requested]
attribute nas-ip-address <WORD>
attribute nas-ipv6-address
attribute operator-name <OPERATOR-NAME>
attribute service-type [framed|login]
```

### Parameters

```
attribute acct-delay-time
```

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| acct-delay-time | Enables support for <i>accounting-delay-time</i> attribute in accounting requests. When enabled, this attribute indicates the number of seconds the client has been trying to send a request to the accounting server. By subtracting this value from the time the packet is received by the server, the system is able to calculate the time of a request-generating event. Note, the network transit time is ignored. This option is disabled by default.<br>Including the acct-delay-time attribute in accounting requests updates the acct-delay-time value whenever the packet is retransmitted, This changes the content of the attributes field, requiring a new identifier and request authenticator. |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
attribute multi-session-id
```

|                       |                                                                                                                                                                                                                                                                                                                                               |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| acct-multi-session-id | Enables support for <i>accounting-multi-session-id</i> attribute. When enabled, it allows linking of multiple related sessions of a roaming client. This option is useful in scenarios where a client roaming between access points sends multiple RADIUS accounting requests to different access points. This option is disabled by default. |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
attribute chargeable-user-identity
```

|                          |                                                                                                    |
|--------------------------|----------------------------------------------------------------------------------------------------|
| chargeable-user-identity | Enables support for <i>chargeable-user-identity</i> attribute. This option is disabled by default. |
|--------------------------|----------------------------------------------------------------------------------------------------|

```
attribute cisco-vsa audit-session-id
```

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cisco-vsa<br>audit-<br>session-id | <p>Configures the CISCO VSA (Vendor Specific Attribute) attribute included in access requests. This feature is disabled by default.</p> <p>This VSA allows CISCO's ISE (Identity Services Engine) to validate a requesting client's network compliance, such as the validity of virus definition files (anti virus software or definition files for an anti-spyware software application).</p> <ul style="list-style-type: none"> <li>• audit-session-id – Includes the audit session ID attribute in access requests</li> </ul> <p>The audit session ID is included in access requests when Cisco ISE is configured as an authentication server.</p> <p><b>Note:</b> If the Cisco VSA attribute is enabled, configure an additional UDP port to listen for dynamic authorization messages from the Cisco ISE server. For more information, see <a href="#">service</a> on page 1245.</p> |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

`attribute framed-ip-address`

|                   |                                                                                                                         |
|-------------------|-------------------------------------------------------------------------------------------------------------------------|
| framed-ip-address | Enables inclusion of framed IP address attribute in access and accounting requests. This option is disabled by default. |
|-------------------|-------------------------------------------------------------------------------------------------------------------------|

`attribute framed-mtu <100-1500>`

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| framed-mtu<br><100-1500> | <p>Configures Framed-MTU attribute used in access requests</p> <p>The Framed-MTU attribute reduces the EAP (Extensible Authentication Protocol) packet size of the RADIUS server. This command is useful in networks where routers and firewalls do not perform fragmentation. EAP authentication uses Framed-MTU to notify the RADIUS server about the MTU negotiation with the client. The RADIUS server communications with the client do not include EAP messages that cannot be delivered over the network.</p> <ul style="list-style-type: none"> <li>• &lt;100-1500&gt; – Specify the Framed-MTU attribute value from 100 - 1500. The default value is 1400.</li> </ul> |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

`attribute location-information [include-always|none|server-requested]`

|                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| location-information<br>[include-always none <br>server-requested] | <p>Enables support for RFC5580 location information attribute, based on the option selected. The options are:</p> <ul style="list-style-type: none"> <li>• include-always – Always includes location information in RADIUS authentication and accounting messages</li> <li>• none – Disables sending of location information in RADIUS authentication and accounting messages. This is the default setting.</li> <li>• server-requested – Includes location information in RADIUS authentication and accounting messages only when requested by the server</li> </ul> <p><b>Note:</b> When enabled, location information is exchanged in authentication and accounting messages.</p> |
|--------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

`attribute nas-ip-address <WORD>`

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| nas-ip-address <WORD> | <p>Enables configuration of an IP address, which is used as the RADIUS attribute 4, NAS-IP-Address, without changing the source IP address in the IP header of the RADIUS packets. If you are using a cluster of small NASs (network access servers) to simulate a large NAS, use this option to improve scalability. The IP address configured using this option allows the NASs to behave as a single RADIUS client from the perspective of the RADIUS server.</p> <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Provide the IPv4 address.</li> </ul> |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

`attribute nas-ipv6-address`

|                  |                                                                                                                                                                                                                                                                        |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| nas-ipv6-address | Enables support for NAS IPv6 address. This option is disabled by default. When enabled, IPv6 addresses are assigned to hosts. The length of IPv4 and IPv6 addresses is 32-bit and 128-bit respectively. Consequently, an IPv6 address requires a larger address space. |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

attribute operator-name <OPERATOR-NAME>

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| operator-name <OPERATOR-NAME> | Enables support for RFC5580 operator name attribute. When enabled, the network operator's name is included in all RADIUS authentication and accounting messages and uniquely identifies the access network owner. This option is disabled by default. <ul style="list-style-type: none"> <li>&lt;OPERATOR-NAME&gt; - Specify the network operator's name (should not exceed 63 characters in length).</li> </ul> |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

attribute service-type [framed|login]

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| service-type [framed login] | Configures the <i>service-type</i> (6) attribute value. This attribute identifies the following: the type of service requested and the type of service to be provided. <ul style="list-style-type: none"> <li>framed - Sets <i>service-type to framed</i> (2) in the authentication packets. When enabled, a framed protocol, PPP (Point-to-Point Protocol) or SLIP (Serial Line Internet Protocol), is started for the client. This is the default setting.</li> <li>login - Sets <i>service-type to login</i> (1) in the authentication packets. When enabled, the client is connected to the host.</li> </ul> |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```

nx9500-6C8809(config-aaa-policy-test)#attribute framed-mtu 110
nx9500-6C8809(config-aaa-policy-test)#show context
aaa-policy test
 accounting server 2 host 172.16.10.10 secret 0 test1 port 1
 accounting server 2 timeout 2 attempts 2
 accounting interim interval 65
 accounting server preference auth-server-number
 attribute framed-mtu 110
nx9500-6C8809(config-aaa-policy-test)#
nx9500-6C8809(config-aaa-policy-test1)#attribute cisco-vsa audit-session-id
nx9500-6C8809(config-aaa-policy-test1)#show context
aaa-policy test1
 attribute cisco-vsa audit-session-id
nx9500-6C8809(config-aaa-policy-test1)#

```

## Related Commands

|    |                                    |
|----|------------------------------------|
| no | Resets values or disables commands |
|----|------------------------------------|

## authentication

Configures user authentication parameters

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000



## Syntax

```
authentication [eap|protocol|server]
authentication eap wireless-client [attempts <1-10>|identity-request-retry-timeout
<10-5000>|
identity-request-timeout <1-60>|retry-timeout-factor <50-200>|timeout <1-60>]
authentication protocol [chap|mschap|mschapv2|pap]
authentication server <1-6> [dscp|host|nac|nai-routing|onboard|proxy-mode|retry-timeout-
factor|timeout]
authentication server <1-6> dscp <0-63>
authentication server <1-6> host <IP/HOSTNAME/HOST-ALIAS> secret [0 <SECRET>|2 <SECRET>|
<SECRET>]
{port <1-65535>}
authentication server <1-6> nac
authentication server <1-6> nai-routing realm-type [prefix|suffix] realm <REALM-NAME>
{strip}
authentication server <1-6> onboard [centralized-controller|controller|self]
authentication server <1-6> proxy-mode [none|through-centralized-controller|
through-controller|through-mint-host <HOSTNAME/MINT-ID>|through-rf-domain-manager]
authentication server <1-6> retry-timeout-factor <50-200>
authentication server <1-6> timeout <1-60> {attempts <1-10>}
```

## Parameters

```
authentication eap wireless-client [attempts <1-10>|identity-request-retry-timeout
<10-5000>|
identity-request-timeout <1-60>|retry-timeout-factor <50-200>|timeout <1-60>]
```

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| eap                                      | Configures EAP authentication parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| wireless-client                          | Configures wireless client's EAP parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| attempts <1-10>                          | Configures the maximum number of attempts allowed to authenticate a wireless client <ul style="list-style-type: none"><li>&lt;1-10&gt; – Specify a value from 1 - 10. The default is 3.</li></ul>                                                                                                                                                                                                                                                                                                                                                                      |
| identity-request-retry-timeout <10-5000> | Configures the interval, in milliseconds, after which an EAP-identity request to the wireless client is retried <ul style="list-style-type: none"><li>&lt;10-5000&gt; – Specify a value from 10 - 5000 milliseconds. The default is 1000 milliseconds.</li></ul>                                                                                                                                                                                                                                                                                                       |
| identity-request-timeout <1-60>          | Configures the timeout, in seconds, after the last EAP-identity request message retry attempt (to allow time to manually enter user credentials) <ul style="list-style-type: none"><li>&lt;1-60&gt; – Specify a value from 1 - 60 seconds. The default is 30 seconds.</li></ul>                                                                                                                                                                                                                                                                                        |
| retry-timeout-factor <50-200>            | Configures the interval between successive EAP retries <ul style="list-style-type: none"><li>&lt;50-200&gt; – Specify a value from 50 - 200. The default is 100.</li></ul> <p>A value of 100 indicates the interval between two consecutive retries remains the same irrespective of the number of retries.</p> <p>A value lesser than 100 indicates the interval between two consecutive retries reduces with each successive retry.</p> <p>A value greater than 100 indicates the interval between two consecutive retries increases with each successive retry.</p> |
| timeout <1-60>                           | Configures the interval, in seconds, between successive EAP-identity request sent to a wireless client <ul style="list-style-type: none"><li>&lt;1-60&gt; – Specify a value from 1 - 60 seconds. The default is 3 seconds.</li></ul>                                                                                                                                                                                                                                                                                                                                   |

```
authentication protocol [chap|mschap|mschapv2|pap]
```

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| protocol [chap mschap mschapv2 pap] | <p>Configures one of the following protocols for non-EAP authentication:</p> <ul style="list-style-type: none"> <li>chap – Uses CHAP (Challenge Handshake Authentication Protocol)</li> <li>mschap – Uses MS-CHAP (Microsoft Challenge Handshake Authentication Protocol)</li> <li>mschapv2 – Uses MS-CHAP version 2</li> <li>pap – Uses PAP (Password Authentication Protocol). This is the default setting.</li> </ul> |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
authentication server <1-6> dscp <0-63>
```

|              |                                                                                                                                                                                                                                                                                                                                                       |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| server <1-6> | <p>Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured.</p> <ul style="list-style-type: none"> <li>&lt;1-6&gt; – Specify the RADIUS server index from 1 - 6.</li> </ul>                                                                                                                                               |
| dscp <0-63>  | <p>Configures the DSCP quality of service parameter generated in RADIUS packets. The DSCP value specifies the class of service provided to a packet, and is represented by a 6-bit parameter in the header of every IP packet.</p> <ul style="list-style-type: none"> <li>&lt;0-63&gt; – Specify the value from 0 - 63. The default is 46.</li> </ul> |

```
authentication server <1-6> host <IP/HOSTNAME/HOST-ALIAS> secret [0 <SECRET>|2 <SECRET>|<SECRET>] {port <1-65535>}
```

|                                         |                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| server <1-6>                            | <p>Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured.</p> <ul style="list-style-type: none"> <li>&lt;1-6&gt; – Specify the RADIUS server index from 1 - 6.</li> </ul>                                                                                                                                                                                     |
| host <IP/HOSTNAME>                      | <p>Sets the RADIUS authentication server's IP address or hostname. You can use a host alias to identify the device hosting the authentication server. Ensure that the host alias is existing and configured.</p>                                                                                                                                                                            |
| secret [0 <SECRET> 2 <SECRET> <SECRET>] | <p>Configures the RADIUS authentication server's secret key. This key is used to authenticate with the RADIUS server.</p> <ul style="list-style-type: none"> <li>0 &lt;SECRET&gt; – Configures a clear text secret</li> <li>2 &lt;SECRET&gt; – Configures an encrypted secret</li> <li>&lt;SECRET&gt; – Specify the secret key. The shared key should not exceed 127 characters.</li> </ul> |
| port <1-65535>                          | <p>Optional. Specifies the RADIUS authentication server's UDP port (this port is used to connect to the RADIUS server)</p> <ul style="list-style-type: none"> <li>&lt;1-65535&gt; – Specify a value from 1 - 65535. The default port is 1812.</li> </ul>                                                                                                                                    |

```
authentication server <1-6> nac
```

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| server <1-6> | <p>Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured.</p> <ul style="list-style-type: none"> <li>&lt;1-6&gt; – Specify the RADIUS server index from 1 - 6.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                     |
| nac          | <p>Enables NAC (Network Access Control) on the RADIUS authentication server identified by the &lt;1-6&gt; parameter.</p> <p>Using NAC, the controller hardware and software grant access to specific network resources. NAC performs a user and client authorization check for resources that do not have a NAC agent. NAC verifies the client's compliance with the controller's security policy. The controller supports only the EAP/802.1x type of NAC. However, the controller also provides a means to bypass NAC authentication for client's that do not have NAC 802.1x support (printers, phones, PDAs, etc.).</p> |

```
accounting server <1-6> nai-routing realm-type [prefix|suffix] realm <REALM-NAME> {strip}
```

|                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| server <1-6>                     | Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured. <ul style="list-style-type: none"> <li>&lt;1-6&gt; – Specifies the RADIUS server index from 1 - 6.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| nai-routing                      | Enables NAI routing. When enabled, AAA servers identify clients using NAI. This option is disabled by default.<br>The NAI is a character string in the format of an e-mail address as either user or user@realm but it need not be a valid e-mail address or a fully qualified domain name. AAA servers identify clients using the NAI. The NAI can be used either in a specific or generic form. The specific form, which must contain the user portion and may contain the @realm portion, identifies a single user. Using the generic form allows all users to be configured on a single command line, irrespective of whether the users are within a realm or not. Each user still needs a unique security association, but these associations can be stored on a AAA server. The original purpose of the NAI was to support roaming between dial up ISPs. With NAI, an ISP does not have the accounts for all of its roaming partners in a single RADIUS database. RADIUS servers can proxy requests to remote servers as need be. |
| realm-type<br>[prefix<br>suffix] | Configures the realm-type used for NAI authentication <ul style="list-style-type: none"> <li>prefix – Sets the realm prefix. For example, in the realm name 'AC\JohnTalbot', the prefix is 'AC' and the user name 'JohnTalbot'.</li> <li>suffix – Sets the realm suffix. For example, in the realm name 'JohnTalbot@AC.org' the suffix is 'AC.org' and the user name is 'JohnTalbot'.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| realm<br><REALM-<br>NAME>        | Sets the realm information used for RADIUS authentication. The realm name should not exceed 64 characters in length. When the wireless controller or access point's RADIUS server receives a request for a user name the server references a table of usernames. If the user name is known, the server proxies the request to the RADIUS server. <ul style="list-style-type: none"> <li>&lt;REALM-NAME&gt; – Sets the realm used for authentication. This value is matched against the user name provided for RADIUS authentication.</li> </ul> <p>Example:</p> <p>Prefix - AC\JohnTalbot</p> <p>Suffix - JohnTalbot@AC.org</p>                                                                                                                                                                                                                                                                                                                                                                                                         |
| strip                            | Optional. Indicates the realm name must be stripped from the user name before sending it to the RADIUS server for authentication. For example, if the complete username is 'AC\JohnTalbot', then with the <i>strip</i> parameter enabled, only the 'JohnTalbot' part of the complete username is sent for authentication. This option is disabled by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

```
authentication server <1-6> onboard [centralized-controller|controller|
self]
```

|                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| server <1-6>                                      | Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured. <ul style="list-style-type: none"> <li>• &lt;1-6&gt; - Specify the RADIUS server index from 1 - 6.</li> </ul>                                                                                                                                                                                                                                                                                                                            |
| onboard [centralized-controller] controller[self] | Selects the onboard RADIUS server for authentication instead of an external host <ul style="list-style-type: none"> <li>• centralized-controller - Configures the server on the centralized controller managing the network</li> <li>• controller - Configures the wireless controller, to which the AP is adopted, as the onboard wireless controller</li> <li>• self - Configures the onboard server on the device (AP or wireless controller) where the client is associated as the onboard wireless controller</li> </ul> |

```
authentication server <1-6> proxy-mode [none|through-centralized-controller|
through-controller|through-mint-host <HOSTNAME/MINT-ID>|through-rf-domain-manager]
```

|                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| server <1-6>                                                                                                                           | Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured. <ul style="list-style-type: none"> <li>• &lt;1-6&gt; - Sets the RADIUS server index between 1 - 6</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| proxy-mode [none] through-centralized-controller  through-controller  through-mint-host <HOSTNAME/MINT-ID>  through-rf-domain-manager] | Configures the mode for proxying a request <ul style="list-style-type: none"> <li>• none - Proxying is not done. The packets are sent directly using the IP address of the device. This is the default setting.</li> <li>• through-centralized-controller - The traffic is proxied through the centralized controller that is configuring and managing the network.</li> <li>• through-controller - The traffic is proxied through the wireless controller configuring this device.</li> <li>• through-mint-host &lt;HOSTNAME/MINT-ID&gt; - The traffic is proxied through a neighboring MiNT device. Provide the device's hostname or MiNT ID.</li> <li>• through-rf-domain-manager - The traffic is proxied through the local RF Domain manager.</li> </ul> |

```
authentication server <1-6> retry-timeout-factor <50-200>
```

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| server <1-6>                  | Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured. <ul style="list-style-type: none"> <li>• &lt;1-6&gt; - Specify the RADIUS server index from 1 - 6.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                      |
| retry-timeout-factor <50-200> | Configures the scaling of timeouts between two consecutive RADIUS authentication retries <ul style="list-style-type: none"> <li>• &lt;50-200&gt; - Specify the scaling factor from 50 - 200. The default is 100.</li> </ul> <p>A value of 100 indicates the interval between two consecutive retries remains the same irrespective of the number of retries.</p> <p>A value lesser than 100 indicates the interval between two consecutive retries reduces with each successive retry.</p> <p>A value greater than 100 indicates the interval between two consecutive retries increases with each successive retry.</p> |

```
authentication server <1-6> timeout <1-60> {attempts <1-10>}
```

|                 |                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| server <1-6>    | Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured <ul style="list-style-type: none"> <li>&lt;1-6&gt; – Specify the RADIUS server index from 1 - 6.</li> </ul>                                                                                                                                                                                                   |
| timeout <1-60>  | Configures the timeout, in seconds, for each request sent to the RADIUS server. This is the time allowed to elapse before another request is sent to the RADIUS server. If a response is received from the RADIUS server within this time, no retry is attempted. <ul style="list-style-type: none"> <li>&lt;1-60&gt; – Specify a value from 1 - 60 seconds. The default is 3 seconds.</li> </ul> |
| attempts <1-10> | Optional. In case of no response from the RADIUS authentication server, this option configures the maximum number of attempts made in contacting the server, before retiring the request <ul style="list-style-type: none"> <li>&lt;1-10&gt; – Specify a value from 1 - 10. The default is 3.</li> </ul>                                                                                          |

### Examples

```

nx9500-6C8809(config-aaa-policy-test)#authentication server 5 host 172.16.10.10 secret 0
test1 port 1
nx9500-6C8809(config-aaa-policy-test)#authentication server 5 timeout 10 attempts 3
nx9500-6C8809(config-aaa-policy-test)#authentication protocol chap
nx9500-6C8809(config-aaa-policy-test)#show context
aaa-policy test
 authentication server 5 host 172.16.10.20 secret 0 test1 port 1
 authentication server 5 timeout 10 attempts 3
 accounting server 2 host 172.16.10.10 secret 0 test1 port 1
 accounting server 2 timeout 2 attempts 2
 authentication protocol chap
 accounting interim interval 65
 accounting server preference auth-server-number
 attribute framed-mtu 110
nx9500-6C8809(config-aaa-policy-test)#

```

### Related Commands

|           |                                                                    |
|-----------|--------------------------------------------------------------------|
| <b>no</b> | Resets authentication server related parameters on this AAA policy |
|-----------|--------------------------------------------------------------------|

### health-check

An AAA server could go offline. When a server goes offline, it is marked as *down*. This command configures the interval after which a server marked as *down* is checked to see if it has come back online and is reachable.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
health-check interval <60-86400>
```

### Parameters

```
health-check interval <60-86400>
```

|                        |                                                                                                                                                                                                                                                     |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| interval<br><60-86400> | Configures an interval (in seconds) after which a down server is checked to see if it is reachable again <ul style="list-style-type: none"> <li>&lt;60-86400&gt; - Specify a value from 60 - 86400 seconds. The default is 3600 seconds.</li> </ul> |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```

nx9500-6C8809(config-aaa-policy-test)#health-check interval 4000
nx9500-6C8809(config-aaa-policy-test)#show context
aaa-policy test
 authentication server 5 host 172.16.10.20 secret 0 test1 port 1
 authentication server 5 timeout 10 attempts 3
 accounting server 2 host 172.16.10.10 secret 0 test1 port 1
 accounting server 2 timeout 2 attempts 2
 authentication protocol chap
 accounting interim interval 65
 accounting server preference auth-server-number
 health-check interval 4000
 attribute framed-mtu 110
nx9500-6C8809(config-aaa-policy-test)#

```

### Related Commands

|    |                                                  |
|----|--------------------------------------------------|
| no | Resets the health-check interval for AAA servers |
|----|--------------------------------------------------|

### mac-address-format

Configures the format MAC addresses are filled in RADIUS request frames

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```

mac-address-format [middle-hyphen|no-delim|pair-colon|pair-hyphen|quad-dot]
case [lower|upper] attributes [all|username-password]

```

#### Parameters

```

mac-address-format [middle-hyphen|no-delim|pair-colon|pair-hyphen|quad-dot]
case [lower|upper] attributes [all|username-password]

```

|               |                                                                                  |
|---------------|----------------------------------------------------------------------------------|
| middle-hyphen | Configures the MAC address format as AABCCDDEEFF                                 |
| no-delim      | Configures the MAC address format as AABCCDDEEFF (without delimiters)            |
| pair-colon    | Configures the MAC address format as AA:BB:CC:DD:EE:FF                           |
| pair-hyphen   | Configures the MAC address display format as AA-BB-CC-DD-EE-FF (default setting) |
| quad-dot      | Configures the MAC address display format as AABB.CCDD.EEFF                      |

|                                    |                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| case [lower upper]                 | Indicates the case the MAC address is formatted <ul style="list-style-type: none"> <li>• lower - Indicates MAC address is in lower case. For example, aa:bb:cc:dd:ee:ff</li> <li>• upper - Indicates MAC address is in upper case. For example, AA:BB:CC:DD:EE:FF (default setting)</li> </ul>                                                     |
| attributes [all username-password] | Configures RADIUS attributes to which this MAC format is applicable <ul style="list-style-type: none"> <li>• all - Applies to all attributes with MAC addresses such as username, password, calling-station-id, and called-station-id</li> <li>• username-password - Applies only to the username and password fields (default setting)</li> </ul> |

### Examples

```

nx9500-6C8809(config-aaa-policy-test)#mac-address-format quad-dot case upper attributes
username-password
nx9500-6C8809(config-aaa-policy-test)#show context
aaa-policy test
 authentication server 5 host 172.16.10.10 secret 0 test1 port 1
 authentication server 5 timeout 10 attempts 3
 accounting server 2 host 172.16.10.10 secret 0 test1 port 1
 accounting server 2 timeout 2 attempts 2
 mac-address-format quad-dot case upper attributes username-password
 authentication protocol chap
 --More--
nx9500-6C8809(config-aaa-policy-test)#

```

### Related Commands

|    |                                                        |
|----|--------------------------------------------------------|
| no | Resets the MAC address format to default (pair-hyphen) |
|----|--------------------------------------------------------|

### *proxy-attribute*

Configures RADIUS server's attribute behavior when proxying through a wireless controller or a RF Domain manager

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```

proxy-attribute [nas-identifier|nas-ip-address]
proxy-attribute [nas-identifier [originator|proxier]]nas-ip-address [none|proxier]]

```

#### Parameters

```

proxy-attribute [nas-identifier [originator|proxier]]nas-ip-address [none|proxier]]

```

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| nas-identifier<br>[originator proxier] | <p>Uses NAS identifier</p> <ul style="list-style-type: none"> <li>• originator – Configures the NAS identifier as the originator of the RADIUS request. The originator could be an AP, or a wireless controller with radio. This is the default setting.</li> <li>• proxier – Configures the proxying device as the NAS identifier. The device could be a controller or a RF Domain manager.</li> </ul> |
| nas-ip-address<br>[none proxier]       | <p>Uses NAS IP address</p> <ul style="list-style-type: none"> <li>• none – NAS IP address attribute is not filled</li> <li>• proxier – NAS IP address is filled by the proxying device. The device could be a controller or a RF Domain manager. This is the default setting.</li> </ul>                                                                                                                |

### Examples

```
nx9500-6C8809(config-aaa-policy-test)#proxy-attribute nas-ip-address proxier
nx9500-6C8809(config-aaa-policy-test)#proxy-attribute nas-identifier originator
```

### Related Commands

|    |                                            |
|----|--------------------------------------------|
| no | Resets RADIUS server's proxying attributes |
|----|--------------------------------------------|

### *server-pooling-mode*

Configures the mode used to select the server from a pool of AAA servers. The available methods are *failover* and *load-balance*.

In the failover scenario, when a configured AAA server goes down, the server with the next higher index takes over for the failed server.

In the load-balance scenario, when a configured AAA server goes down, the remaining servers distribute the load amongst themselves.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
server-pooling-mode [failover|load-balance]
```

### Parameters

```
server-pooling-mode [failover|load-balance]
```

|              |                                                                                                                                                                                      |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| failover     | Sets the pooling mode to failover. This is the default setting. When a configured AAA server fails, the server with the next higher index takes over the failed server's load.       |
| load-balance | Sets the pooling mode to load balancing. When a configured AAA server fails, all servers in the pool share the failed server's load, transmitting requests in a round-robin fashion. |



## Examples

```
nx9500-6C8809(config-aaa-policy-test)#server-pooling-mode load-balance
nx9500-6C8809(config-aaa-policy-test)#show context
aaa-policy test
 authentication server 5 host 172.16.10.10 secret 0 test2 port 1
 authentication server 5 timeout 10 attempts 3
 accounting server 2 host 172.16.10.10 secret 0 test1 port 1
 server-pooling-mode load-balance
 mac-address-format quad-dot case upper attributes username-password
 accounting server preference auth-server-number
 health-check interval 4000
nx9500-6C8809(config-aaa-policy-test)#
```

## Related Commands

|                                                                                                  |
|--------------------------------------------------------------------------------------------------|
| <code>no</code> Resets the method of selecting a server, from the pool of configured AAA servers |
|--------------------------------------------------------------------------------------------------|

## use

Associates a NAC (Network Access Control) list with this AAA policy. When associated only the set of configured devices to allowed use of the configured AAA servers.

For more information on creating a NAC list, see [nac-list](#).

## Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
use nac-list <NAC-LIST-NAME>
```

## Parameters

```
use nac-list <NAC-LIST-NAME>
```

|                                             |                                                                                                                                                                                                  |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>nac-list &lt;NAC-LIST-NAME&gt;</code> | Associates a NAC list with this AAA policy <ul style="list-style-type: none"><li>• <code>&lt;NAC-LIST-NAME&gt;</code> - Specify the NAC list name (should be existing and configured).</li></ul> |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-aaa-policy-test)#use nac-list test1
nx9500-6C8809(config-aaa-policy-test)#show context
aaa-policy test
 authentication server 5 host 172.16.10.10 secret 0 test1 port 1
 authentication server 5 timeout 10 attempts 3
 accounting server 2 host 172.16.10.10 secret 0 test1 port 1
 server-pooling-mode load-balance
 mac-address-format quad-dot case upper attributes username-password
 accounting server preference auth-server-number
 health-check interval 4000
 use nac-list test1
nx9500-6C8809(config-aaa-policy-test)#
```

## Related Commands

|                       |                                             |
|-----------------------|---------------------------------------------|
| <code>no</code>       | Dissociates a NAC list from this AAA policy |
| <code>nac-list</code> | Creates a NAC list                          |

`no`

Removes this AAA policy settings or reverts them to default values

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
no [accounting|attribute|authentication|health-check|mac-address-format|proxy-attribute|
server-pooling-mode|use]
no accounting interim interval
no accounting server preference
no accounting server <1-6> {dscp/nai-routing/proxy-mode/retry-timeout-factor/timeout}
no accounting type
no attribute [acct-delay-time|acct-multi-session-id|chargeable-user-identity|
cisco-vsa audit-session-id|framed-ip-address|framed-mtu|location-information|nas-ipv6-
address|
operator-name|service-type]
no authentication [eap|protocol|server]
no authentication eap wireless-client [attempts|identity-request-retry-timeout|
identity-request-timeout|retry-timeout-factor|timeout]
no authentication protocol
no authentication server <1-6> {dscp/nac/nai-routing/proxy-mode/retry-timeout-factor/
timeout}
no health-check interval
no mac-address-format
no proxy-attribute [nas-identifier|nas-ip-address]
no server-pooling-mode
no use nac-list
```

### Parameters

`no <PARAMETERS>`

|                                    |                                                                |
|------------------------------------|----------------------------------------------------------------|
| <code>no &lt;PARAMETERS&gt;</code> | Removes or reverts to default the selected AAA policy settings |
|------------------------------------|----------------------------------------------------------------|

### Examples

The following example shows the AAA policy 'test' settings before the 'no' commands are executed:

```
nx9500-6C8809(config-aaa-policy-test)#show context
aaa-policy test
 authentication server 5 host 172.16.10.10 secret 0 test1 port 1
 authentication server 5 timeout 10 attempts 3
 accounting server 2 host 172.16.10.10 secret 0 test1 port 1
 accounting server 2 timeout 2 attempts 2
 mac-address-format quad-dot case upper attributes username-password
 authentication protocol chap
 accounting interim interval 65
 accounting server preference auth-server-number
```

---

```
health-check interval 4000
attribute framed-mtu 110
nx9500-6C8809(config-aaa-policy-test)#
nx9500-6C8809(config-aaa-policy-test)#no accounting server 2 timeout 2
nx9500-6C8809(config-aaa-policy-test)#no accounting interim interval
nx9500-6C8809(config-aaa-policy-test)#no health-check interval
nx9500-6C8809(config-aaa-policy-test)#no attribute framed-mtu
nx9500-6C8809(config-aaa-policy-test)#no authentication protocol
```

The following example shows the AAA policy 'test' settings after the 'no' commands are executed:

```
nx9500-6C8809(config-aaa-policy-test)#show context
aaa-policy test
authentication server 5 host 172.16.10.10 secret 0 test1 port 1
authentication server 5 timeout 10 attempts 3
accounting server 2 host 172.16.10.10 secret 0 test1 port 1
mac-address-format quad-dot case upper attributes username-password
accounting server preference auth-server-number
health-check interval 4000
nx9500-6C8809(config-aaa-policy-test)#
```

# AUTO PROVISIONING POLICY

## AUTO-PROVISIONING-POLICY

---

This topic summarizes the auto provisioning policy commands in the CLI command structure.

Wireless devices can adopt and manage other wireless devices. For example, a wireless controller can adopt multiple access points. When a device is adopted, the device configuration is provisioned by the adopting device. Since multiple configuration policies are supported, an adopting device uses auto provisioning policies to determine which configuration policies are applied to an adoptee based on its properties. For example, a configuration policy could be assigned based on MAC address, IP address, CDP snoop strings, etc.

Auto provisioning or adoption is the process by which an access point discovers controllers in the network, identifies the most desirable controller, associates with the identified controller, and optionally obtains an image upgrade, obtains its configuration and considers itself provisioned.

At adoption, an access point solicits and receives multiple adoption responses from controllers available on the network. These adoption responses contain loading policy information the access point uses to select the optimum controller for adoption. An auto-provisioning policy maps a new AP to a profile and RF Domain based on various parameters related to the AP and where it is connected. By default a new AP will be mapped to the default profile and default RF Domain. Modify existing auto-provisioning policies or create a new one as needed to meet the configuration requirements of a device.

An auto-provisioning policy enables an administrator to define rules for the supported access points capable of being adopted by a controller. The policy determines which configuration policies are applied to an adoptee based on its properties. For example, a configuration policy could be assigned based on MAC address, IP address, CDP (cisco discovery protocol) snoop strings, etc. Once created an auto provisioning policy can be used in profiles or device configuration objects. The policy contains a set of rules (ordered by precedence) that either deny or allow adoption based on potential adoptee properties and a catch-all variable that determines if the adoption should be allowed when none of the rules is matched. All rules (both deny and allow) are evaluated sequentially starting with the rule with the lowest precedence. The evaluation stops as soon as a rule has been matched, no attempt is made to find a better match further down in the set.

For example,

```
rule #1 adopt ap7161 10 profile default vlan 10
rule #2 adopt ap6562 20 profile default vlan 20
rule #3 adopt ap7161 30 profile default serial-number
rule #4 adopt ap7161 40 p d mac aa bb
```

AP 7161 L2 adoption, VLAN 10 - will use rule #1

AP 7161 L2 adoption, VLAN 20 - will not use rule #2 (wrong type), may use rule #3 if the serial number matched, or rule #4

If aa<= MAC <= bb, or else default.

With the implementation of the HM hierarchically managed network, the auto-provisioning policy has been modified to enable controllers to adopt other controllers in addition to access points.

The new WiNG HM network defines a three-tier structure, consisting of multiple wireless sites managed by a single NOC (Network Operations Center) controller, The NOC controller constitutes the first and the site controllers constitute the second tier of the hierarchy. The site controllers in turn adopt and manage access points that form the third tier of the hierarchy.

All adopted devices (access points and second-level controllers) are referred to as the 'adoptee'. The adopting devices are the 'adopters'.

A controller cannot be configured as an adoptee and an adopter simultaneously. In other words, a controller can either be an adopter (adopts another controller) or an adoptee (is adopted by another controller). Therefore, a site controller, which has been adopted by a NOC controller, cannot adopt another controller.

A controller should be configured to specify the device types (APs and/or controllers) that it can adopt. For more information on configuring the adopted-device types for a controller, see [controller](#) on page 918.

---

#### Note

The adoption capabilities of a controller depends on:



- Whether the controller is deployed at the NOC or site
  - A NOC controller can adopt site controllers and access points
  - A site controller can adopt access points only
- The controller device type, which determines the number and type of devices it can adopt

---

Use the (config) instance to configure auto-provisioning-policy. To navigate to the auto-provisioning-policy configuration instance, use the following command:

```
<DEVICE>(config)#auto-provisioning-policy <POLICY-NAME>
nx9500-6C8809(config)#auto-provisioning-policy test
nx9500-6C8809(config-auto-provisioning-policy-test)#?
Auto-Provisioning Policy Mode commands:
 adopt Add rule for device adoption
 auto-create-rfd-template When RF Domain specified by the matching rule
 template does not exist create new RF Domain
 automatically
 default-adoption Adopt devices even when no matching rules are
 found. Assign default profile and default
 rf-domain
 deny Add rule to deny device adoption
 evaluate-always Set the flag to evaluate the policy everytime,
 regardless of previous adoption status
 no Negate a command or set its defaults
 redirect Add rule to redirect device adoption
 upgrade Add rule for device upgrade

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
```

```

show Show running system information
write Write running configuration to memory or terminal
nx9500-6C8809(config-auto-provisioning-policy-test)#

```

## auto-provisioning-policy-commands

The following table summarizes auto provisioning policy configuration commands:

*Table: Auto Provisioning Policy Configuration Commands*

| Command                       | Description                                                                                         |
|-------------------------------|-----------------------------------------------------------------------------------------------------|
| <code>adopt</code>            | Adds a permit adoption rule                                                                         |
| <code>default-adoption</code> | Adopts devices even when no matching rules are found. Assigns default profile and default RF Domain |
| <code>deny</code>             | Adds a deny adoption rule                                                                           |
| <code>no</code>               | Negates a command or reverts settings to their default                                              |
| <code>redirect</code>         | Adds a rule redirecting device adoption to a specified controller within the system                 |
| <code>upgrade</code>          | Adds a device upgrade rule to this auto provisioning policy                                         |
| <code>evaluate-always</code>  | Sets the flag value                                                                                 |



### Note

For more information on common commands (clscr, commit, help, revert, service, show, write, and exit), see [COMMON COMMANDS](#) on page 640.



### Note

The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (\_) character. In other words, the name of a device cannot contain an underscore.

## *adopt*

Adds device adoption rules to the Auto Provisioning Policy

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```

adopt [anyap | ap6522 | ap6562 | ap71xx | ap7502 | ap7522 | ap7532 | ap7562 | ap7602 | ap7612 | ap7622 | ap7632 |
ap7662 |
ap81xx | ap8432 | ap8533 | rfs4000 | nx5500 | nx75xx | nx9000 | vx9000 | nx9600]
adopt [anyap | ap6522 | ap6562 | ap71xx | ap7502 | ap7522 | ap7532 | ap7562 | ap7602 | ap7612 | ap7622 | ap7632 |
ap7662 |

```

```

ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx9000|vx9000|nx9600] precedence <1-10000>
[profile|rf-domain]
adopt [anyap|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7632|ap7662|
ap7662|
ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx9000|vx9000|nx9600] precedence <1-10000>
[profile <DEVICE-PROFILE-NAME>|rf-domain <RF-DOMAIN-NAME>] [any|area|cdp-match|dhcp-option|
floor|
fqdn|ip|ipv6|lldp-match|mac|model-number|rf-domain|serial-number|vlan]
adopt [anyap|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|
ap7662|
ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx9000|vx9000|nx9600] precedence <1-10000>
[profile <DEVICE-PROFILE-NAME>|rf-domain <RF-DOMAIN-NAME>] any
adopt [anyap|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|
ap7662|
ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx9000|vx9000|nx9600] precedence <1-10000>
[profile <DEVICE-PROFILE-NAME>|rf-domain <RF-DOMAIN-NAME>] [area <AREA-NAME>|
cdp-match <LOCATION-SUBSTRING>|dhcp-option <DHCP-OPTION>|floor <FLOOR-NAME>|fqdn <FQDN>|
ip [<START-IP> <END-IP>|<IP/MASK>]|ipv6 [<START-IP> <END-IP>|<IP/MASK>]|lldp-match <LLDP-
STRING>|
mac <START-MAC> {<END-MAC>}|model-number <MODEL-NUMBER>|serial-number <SERIAL-NUMBER>|
rf-domain <RF-DOMAIN-NAME>|vlan <VLAN-ID>]

```

## Parameter

```

adopt [anyap|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|
ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx9000|vx9000|nx9600] precedence
<1-10000>
[profile <DEVICE-PROFILE-NAME>|rf-domain <RF-DOMAIN-NAME>] any

```

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| adopt                         | Adds an adopt device rule. The rule applies to the selected device types. Specify the device type and assign a precedence to the rule.<br>The different device types are:<br>AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533, RFS 4000, NX 5500, NX 75XX, NX 95XX, NX 96XX, and VX 9000.                                                                                                                                                                                                                              |
| precedence <1-10000>          | Sets the rule precedence from 1 - 10000. A rule with a lower value has a higher precedence.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| profile <DEVICE-PROFILE-NAME> | Sets the device profile for this provisioning policy. The selected device profile must be appropriate for the device being provisioned. For example, use an AP 7502 device profile for an AP 7502. Using an inappropriate device profile can result in unpredictable results. Provide a device profile name.<br>Provide a device profile name (should be existing and configured). Or a template with appropriate substitution tokens, such as 'campus- $\$$ MODEL[1:6]', 'FQDN[1:4]-indoor'. Refer to <a href="#">Usage Guidelines</a> for the different types of built in tokens available in the system. |

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| rf-domain <RF-DOMAIN-NAME> | <p>Sets the RF Domain for this auto provisioning policy. The provisioning policy is only applicable to devices that try to become a part of the specified RF Domain. Provide the full RF Domain name OR use a string alias to identify the RF Domain.</p> <p>Provide the full RF Domain name or an alias (should be existing and configured). Or a template with appropriate substitution tokens, such as '\$CDP[1:7]', '\$DNS-SUFFIX[1:5]'. Refer to <a href="#">Usage Guidelines</a> for the different types of built in tokens available in the system.</p> <p>Use the built-in string alias or a user-defined string alias. String aliases allow you to configure APs in the same RF Domain as the adopting controller. A string alias maps a name to an arbitrary string value, for example, 'alias string \$DOMAIN test.example_company.com'. In this example, the string-alias \$DOMAIN is mapped to the string: <i>test.example_company.com</i>. For more information, see <a href="#">alias</a>.</p> |
| any                        | Indicates any device. Any device seeking adoption is adopted.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

```
adopt [anyap|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|
ap7622|ap7632|ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx9000|vx9000|nx9600]
precedence <1-10000> [profile <DEVICE-PROFILE-NAME>|rf-domain <RF-DOMAIN-NAME>]
[area <AREA-NAME>|cdp-match <LOCATION-SUBSTRING>|dhcp-option <DHCP-OPTION>|floor <FLOOR-
NAME>|
fqdn <FQDN>|ip [<START-IP> <END-IP>|<IP/MASK>]|ipv6 [<START-IP> <END-IP>|<IP/MASK>]|
lldp-match <LLDP-STRING>|mac <START-MAC> {<END-MAC>}|model-number <MODEL-NUMBER>|
serial-number <SERIAL-NUMBER>|rf-domain <RF-DOMAIN-NAME>|vlan <VLAN-ID>]
```

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| adopt                         | <p>Adds an adopt device rule. The rule applies to the selected device types. Specify the device type and assign a precedence to the rule.</p> <p>The different device types are:<br/>AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533, RFS 4000, NX 5500, NX 75XX, NX 95XX, NX 96XX, and VX 9000.</p> <p><b>Note:</b> Use the 'anyap' option to auto provision any AP regardless of its model type.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| precedence <1-10000>          | Sets the rule precedence. A rule with a lower value has a higher precedence.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| profile <DEVICE-PROFILE-NAME> | <p>Sets the device profile for this provisioning policy. The selected device profile must be appropriate for the device being provisioned. For example, use an AP 7502 device profile for an AP 7502. Using an inappropriate device profile can result in unpredictable results. Provide a device profile name.</p> <p>Provide a device profile name (should be existing and configured). Or a template with appropriate substitution tokens, such as 'campus-\$MODEL[1:6]', 'FQDN[1:4]-indoor'. Refer to <a href="#">Usage Guidelines</a> for the different types of built in tokens available in the system.</p>                                                                                                                                                                                                                                                                                                                                                                                                         |
| rf-domain <RF-DOMAIN-NAME>    | <p>Sets the RF Domain for this auto provisioning policy. The provisioning policy is only applicable to devices that try to become a part of the specified RF Domain. Provide the full RF Domain name OR use a string alias to identify the RF Domain.</p> <p>Provide the full RF Domain name or an alias (should be existing and configured). Or a template with appropriate substitution tokens, such as '\$CDP[1:7]', '\$DNS-SUFFIX[1:5]'. Refer to <a href="#">Usage Guidelines</a> for the different types of built in tokens available in the system.</p> <p><b>Note:</b> Use the built-in string alias or a user-defined string alias. String aliases allow you to configure APs in the same RF Domain as the adopting controller. A string alias maps a name to an arbitrary string value, for example, 'alias string \$DOMAIN test.example_company.com'. In this example, the string-alias \$DOMAIN is mapped to the string: <i>test.example_company.com</i>. For more information, see <a href="#">alias</a>.</p> |
| area <AREA-NAME>              | <p>Matches the area of deployment. This option is not applicable to the 'rf-domain' parameter.</p> <ul style="list-style-type: none"> <li>&lt;AREA-NAME&gt; - Enter a 64 character maximum deployment area name assigned to this policy. Devices with matching area names are adopted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |



|                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cdp-match<br><LOCATION-SUBSTRING>       | Matches a substring in a list of CDP snoop strings (case insensitive). For example, if an access point snooped 3 devices: controller1.example.com, controller2.example.com, and controller3.example.com, 'controller1', 'example', 'example.com', are examples of the substrings that will match. <ul style="list-style-type: none"> <li>• &lt;LOCATION-SUBSTRING&gt; – Specify the value to match. Devices matching the specified value are adopted.</li> </ul>                                                                                                                                           |
| dhcp-option<br><DHCP-OPTION>            | Matches the value found in DHCP vendor option 191 (case insensitive). DHCP vendor option 191 can be setup to communicate various configuration parameters to an AP. The value of the option in a string in the form of tag=value separated by a semicolon, for example 'tag1=value1;tag2=value2;tag3=value3'. The access point includes the value of tag 'rf-domain', if present. <ul style="list-style-type: none"> <li>• &lt;DHCP-OPTION&gt; – Specify the DHCP option. Devices matching the specified value are adopted.</li> </ul>                                                                     |
| floor <FLOOR-NAME>                      | Matches the floor name. This option is not applicable to the 'rf-domain' parameter. <ul style="list-style-type: none"> <li>• &lt;FLOOR-NAME&gt; – Enter a 32 character maximum deployment floor name assigned to this policy. Devices with matching floor names are adopted.</li> </ul>                                                                                                                                                                                                                                                                                                                    |
| fqdn <FQDN>                             | Matches a substring to the FQDN (Fully Qualified Domain Name) of a device (case insensitive) FQDN is a domain name that specifies its exact location in the DNS hierarchy. It specifies all domain levels, including its top-level domain and the root domain. This parameter allows a device to adopt based on its FQDN value. <ul style="list-style-type: none"> <li>• &lt;FQDN&gt; – Specify the FQDN name. Devices matching the specified value are adopted.</li> </ul>                                                                                                                                |
| ip [<START-IP><br><END-IP>] <IP/MASK>   | Adopts a device if its IP address matches the specified IPv4 address or is within the specified IP address range. Or if the device is a part of the specified subnet. <ul style="list-style-type: none"> <li>• &lt;START-IP&gt; – Specify the first IPv4 address in the range. <ul style="list-style-type: none"> <li>• &lt;END-IP&gt; – Specify the last IPv4 address in the range.</li> </ul> </li> <li>• &lt;IP/MASK&gt; – Specify the IPv4 subnet and mask to match against the device's IP address.</li> </ul>                                                                                        |
| ipv6 [<START-IP><br><END-IP>] <IP/MASK> | Adopts a device if its IP address matches the specified IPv6 address or is within the specified IP address range. Or if the device is a part of the specified subnet. <ul style="list-style-type: none"> <li>• &lt;START-IP&gt; – Specify the first IPv6 address in the range. <ul style="list-style-type: none"> <li>• &lt;END-IP&gt; – Specify the last IPv6 address in the range.</li> </ul> </li> <li>• &lt;IP/MASK&gt; – Specify the IPv6 subnet and mask to match against the device's IPv6 address.</li> </ul>                                                                                      |
| lldp-match<br><LLDP-STRING>             | Matches a substring in a list of LLDP (Link Layer Discovery Protocol) snoop strings (case insensitive). For example, if an Access Point snooped 3 devices: controller1.example.com, controller2.example.com and controller3.example.com,'controller1', 'example', 'example.com', are substrings match. LLDP is a vendor neutral link layer protocol that advertises a network device's identity, capabilities, and neighbors on a local area network. <ul style="list-style-type: none"> <li>• &lt;LLDP-STRING&gt; – Specify the LLDP string. Devices matching the specified value are adopted.</li> </ul> |
| mac <START-MAC> {<END-MAC>}             | Adopts a device if its MAC address matches the specified MAC address or is within the specified MAC address range <START-MAC> – Specify the first MAC address in the range. Provide this MAC address if you want to match for a single device. <ul style="list-style-type: none"> <li>• &lt;END-MAC&gt; – Optional. Specify the last MAC address in the range.</li> </ul>                                                                                                                                                                                                                                  |
| model-number<br><MODEL-NUMBER>          | Adopts a device if its model number matches <MODEL-NUMBER> <ul style="list-style-type: none"> <li>• &lt;MODEL-NUMBER&gt; – Specify the model number to match.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                   |

|                                      |                                                                                                                                                                                 |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| serial-number<br><SERIAL-<br>NUMBER> | Adopts a device if its serial number matches <SERIAL-NUMBER><br><ul style="list-style-type: none"> <li>• &lt;SERIAL-NUMBER&gt; - Specify the serial number to match.</li> </ul> |
| vlan <VLAN-ID>                       | Adopts a device if its VLAN matches <VLAN-ID><br><ul style="list-style-type: none"> <li>• &lt;VLAN-ID&gt; - Specify the VLAN ID.</li> </ul>                                     |

**Usage Guidelines: Built-in Tokens & Alias**

Following are the built-in tokens that can be used to identify the devices to adopt:

- \$FQDN - references FQDN of adopting device
- \$CDP - references CDP Device Id of the wired switch to which adopting device is connected
- \$LLDP - references LLDP System Name of wired switch to which adopting device is connected
- \$DHCP - references DHCP Option Value received by the adopting device
- \$SN - references SERIAL NUMBER of adopting device
- \$MODEL - references MODEL NUMBER of adopting device
- \$DNS-SUFFIX - references FQDN excluding the hostname of the adopting device
- \$CDP-SUFFIX - references CDP excluding the hostname of the adopting device
- \$LLDP-SUFFIX - references LLDP excluding the hostname of the adopting device

Following is the built-in alias that can be used to identify the RF Domain of devices to adopt:

- \$AUTO-RF-DOMAIN - rf-domain of adopting device

**Examples**

```
rfs4000-229D58(config-auto-provisioning-policy-test)#adopt ap8432 precedence 5 profile
default-ap8432 rf-domain TechPubs vlan 1
rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 adopt ap8432 precedence 5 profile default-ap8432 rf-domain TechPubs vlan 1
rfs4000-229D58(config-auto-provisioning-policy-test)#
rfs4000-229D58(config-auto-provisioning-policy-test)#show wireless ap configured

 IDX NAME MAC PROFILE RF-DOMAIN ADOPTED-BY

 1 ap8432-711728 B4-C7-99-71-17-28 default-ap8432 default 00-23-68-22-9D-58

rfs4000-229D58(config-auto-provisioning-policy-test)#
```

**Related Commands**

|    |                                                                 |
|----|-----------------------------------------------------------------|
| no | Removes an adopt device rule from this Auto Provisioning Policy |
|----|-----------------------------------------------------------------|

*auto-create-rfd-template*

Enables auto creation of an RF Domain:

- when tokens are used to select the RF Domain to apply to devices matching the adoption criteria, and
- the token-specified RF Domain does not exist.

During device adoption, if the token-specified RF Domain (configured using the 'adopt' rule) is not found, the system auto creates a new RF Domain based on an existing RF Domain template specified using this command. This option is disabled by default.



## Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
auto-create-rfd-template <RF-DOMAIN-NAME>
```

## Parameters

```
auto-create-rfd-template <RF-DOMAIN-NAME>
```

|                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| auto-create-rfd-template <RF-DOMAIN-NAME> | <p>Auto creates a new RF Domain based on an existing RF Domain template</p> <ul style="list-style-type: none"><li>• &lt;RF-DOMAIN-NAME&gt; – Specify the RF Domain name (should be existing and configured). The new RF Domain created is saved with the token name specified in the 'adopt' command.</li></ul> <p><b>Note:</b> For more information on configuring tokens, see <a href="#">Usage Guidelines: Built-in Tokens &amp; Alias</a>.</p> |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

The following example configures an adopt rule for adopting any AP7532 and applying an RF Domain matching the token "\$MODEL[1:5]" to the adopted AP:

```
nx9500-6C8809(config-auto-provisioning-policy-test)#adopt ap7532 precedence 20
rf-domain $MODEL[1:5] any
nx9500-6C8809(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 adopt ap7532 precedence 20 rf-domain $MODEL[1:5] any
nx9500-6C8809(config-auto-provisioning-policy-test)#
```

The following example enables auto creation of an RF Domain using an existing RF Domain 'rfd-AP' as template:

- RF Domain name "AP-75": Applicable to any AP 7532

```
nx9500-6C8809(config-auto-provisioning-policy-test)#auto-create-rfd-template AP-75
nx9500-6C8809(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 adopt ap7532 precedence 20 any
 auto-create-rfd-template rfd-AP
nx9500-6C8809(config-auto-provisioning-policy-test)#
```
- As per the above configurations, when an AP 7532 comes up for first-time adoption, the system:
  - Checks for an RF Domain matching the options provided in the 'adopt' rule, and if not found
  - auto creates the RF Domain only if:
    - A token is specified in the 'adopt' rule. For example, \$MODEL[1:5], and
    - the 'auto-create-rfd-template' option is configured
  - Uses the 'RF Domain' specified in the auto-create-rfd-template command as a template. Therefore, the specified RF Domain should be existing and configured.
  - Applies the new RF Domain to the AP.

## Related Commands

|                 |                                        |
|-----------------|----------------------------------------|
| no on page 1353 | Disables auto creation of an RF Domain |
|-----------------|----------------------------------------|

## default-adoption

Adopts devices, even when no matching rules are defined, and assigns a default profile and default RF Domain to the adopted device

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
default-adoption
```

### Parameters

None

### Examples

```
rfs4000-229D58(config-auto-provisioning-policy-test)#default-adoption
rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 default-adoption
 adopt ap8432 precedence 5 profile default-ap8432 rf-domain TechPubs vlan 1
rfs4000-229D58(config-auto-provisioning-policy-test)#
```

### Related Commands

|                                                                                |
|--------------------------------------------------------------------------------|
| <code>no</code> Disables adoption of devices when matching rules are not found |
|--------------------------------------------------------------------------------|

## deny

Adds deny device adoption rules to the Auto Provisioning Policy

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
deny [anyap|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|
ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx9000|vx9000|nx9600]
deny [anyap|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|
ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx9000|vx9000|nx9600] precedence
<1-10000>
[any|cdp-match|dhcp-option|fqdn|ip|ipv6|lldp-match|mac|model-number|serial-number|vlan]
deny [anyap|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|
ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx9000|vx9000|nx9600]
precedence <1-10000> any
deny [anyap|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|
ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx9000|vx9000|nx9600] precedence
<1-10000>
```

```
[cdp-match <LOCATION-SUBSTRING>|dhcp-option <DHCP-OPTION>|fqdn <FQDN>|ip [<START-IP> <END-IP>|<IP/MASK>]|ipv6 [<START-IP> <END-IP>|<IP/MASK>]|lldp-match <LLDP-STRING>|mac <START-MAC> {<END-MAC>}|model-number <MODEL-NUMBER>|serial-number <SERIAL-NUMBER>|vlan <VLAN-ID>]
```

## Parameters

```
deny [anyap|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx9000|vx9000|nx9600] precedence <1-10000> any
```

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| deny                 | <p>Adds a deny adoption rule. The rule applies to the selected device types. Specify the device type and assign a precedence to the rule.</p> <p>The different device types are:<br/>AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533, RFS 4000, NX 5500, NX 75XX, NX 95XX, NX 96XX, and VX 9000.</p> <p><b>Note:</b> Use the 'anyap' option to auto provision any AP regardless of its model type.</p> |
| precedence <1-10000> | Sets the rule precedence. A rule with a lower value has a higher precedence.                                                                                                                                                                                                                                                                                                                                                                                                                 |
| any                  | Indicates any device. Any device seeking adoption is denied adoption.                                                                                                                                                                                                                                                                                                                                                                                                                        |

```
deny [anyap|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx9000|vx9000|nx9600] precedence <1-10000> [cdp-match <LOCATION-SUBSTRING>|dhcp-option <DHCP-OPTION>|fqdn <FQDN>|ip [<START-IP> <END-IP>|<IP/MASK>]|ipv6 [<START-IP> <END-IP>|<IP/MASK>]|lldp-match <LLDP-STRING>|mac <START-MAC> {<END-MAC>}|model-number <MODEL-NUMBER>|serial-number <SERIAL-NUMBER>|vlan <VLAN-ID>]
```

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| adopt                          | <p>Adds a deny adoption rule. The rule applies to the selected device types. Specify the device type and assign a precedence to the rule.</p> <p>The different device types are:<br/>AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533, RFS 4000, NX 5500, NX 75XX, NX 95XX, NX 96XX, and VX 9000.</p> <p><b>Note:</b> Use the 'anyap' option to auto provision any AP regardless of its model type.</p> |
| precedence <1-10000>           | <p>Sets the rule precedence. A rule with a lower value has a higher precedence.</p> <p>After specifying the rule precedence, specify the match criteria. Devices matching the specified criteria are denied adoption.</p>                                                                                                                                                                                                                                                                    |
| cdp-match <LOCATION-SUBSTRING> | <p>Matches a substring in a list of CDP snoop strings (case insensitive). For example, if an access point snooped 3 devices: controller1.example.com, controller2.example.com, and controller3.example.com, 'controller1', 'example', 'example.com', are examples of the substrings that will match.</p> <ul style="list-style-type: none"> <li>&lt;LOCATION-SUBSTRING&gt; - Specify the value to match. Devices matching the specified value are denied adoption.</li> </ul>                |

|                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dhcp-option<br><DHCP-OPTION>                 | <p>Matches the value found in DHCP vendor option 191 (case insensitive). DHCP vendor option 191 can be setup to communicate various configuration parameters to an AP. The value of the option in a string in the form of tag=value separated by a semicolon, for example 'tag1=value1;tag2=value2;tag3=value3'. The access point includes the value of tag 'rf-domain', if present.</p> <ul style="list-style-type: none"> <li>• &lt;DHCP-OPTION&gt; – Specify the DHCP option value to match. Devices matching the specified value are denied adoption.</li> </ul>                        |
| fqdn <FQDN>                                  | <p>Matches a substring to the FQDN of a device (case insensitive)<br/>FQDN is a domain name that specifies its exact location in the DNS hierarchy. It specifies all domain levels, including its top-level domain and the root domain.</p> <ul style="list-style-type: none"> <li>• &lt;FQDN&gt; – Specify the FQDN. Devices matching the specified value are denied adoption.</li> </ul>                                                                                                                                                                                                  |
| ip [<START-IP><br><END-IP>] <IP/<br>MASK>]   | <p>Denies adoption if a device's IP address matches the specified IPv4 address or is within the specified IP address range</p> <ul style="list-style-type: none"> <li>• &lt;START-IP&gt; – Specify the first IPv4 address in the range. <ul style="list-style-type: none"> <li>• &lt;END-IP&gt; – Specify the last IPv4 address in the range.</li> </ul> </li> <li>• &lt;IP/MASK&gt; – Specify the IPv4 subnet and mask to match against the device's IP address.</li> </ul>                                                                                                                |
| ipv6 [<START-IP><br><END-IP>] <IP/<br>MASK>] | <p>Denies adoption if a device's IPv6 address matches the specified IP address or is within the specified IP address range</p> <ul style="list-style-type: none"> <li>• &lt;START-IP&gt; – Specify the first IPv6 address in the range. <ul style="list-style-type: none"> <li>• &lt;END-IP&gt; – Specify the last IPv6 address in the range.</li> </ul> </li> <li>• &lt;IP/MASK&gt; – Specify the IPv6 subnet and mask to match against the device's IPv6 address.</li> </ul>                                                                                                              |
| lldp-match<br><LLDP-STRING>                  | <p>Matches a substring in a list of LLDP snoop strings (case insensitive). For example, if an Access Point snooped 3 devices: controller1.example.com, controller2.example.com and controller3.example.com, 'controller1', 'example', 'example.com', are substrings match. LLDP is a vendor neutral link layer protocol that advertises a network device's identity, capabilities, and neighbors on a local area network.</p> <ul style="list-style-type: none"> <li>• &lt;LLDP-STRING&gt; – Specify the LLDP string. Devices matching the specified values are denied adoption.</li> </ul> |
| mac <START-<br>MAC> {<END-<br>MAC>}          | <p>Denies adoption if a device's MAC address matches the specified MAC address or is within the specified MAC address range</p> <ul style="list-style-type: none"> <li>• &lt;START-MAC&gt; – Specify the first MAC address in the range. Provide this MAC address if you want to match for a single device.</li> <li>• &lt;END-MAC&gt; – Optional. Specify the last MAC address in the range.</li> </ul>                                                                                                                                                                                    |
| model-number<br><MODEL-<br>NUMBER>           | <p>Denies adoption if a device's model number matches &lt;MODEL-NUMBER&gt;</p> <ul style="list-style-type: none"> <li>• &lt;MODEL-NUMBER&gt; – Specify the model number to match.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                |
| serial-number<br><SERIAL-<br>NUMBER>         | <p>Denies adoption if a device's serial number matches &lt;SERIAL-NUMBER&gt;</p> <ul style="list-style-type: none"> <li>• &lt;SERIAL-NUMBER&gt; – Specify the serial number to match.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                            |
| vlan <VLAN-ID>                               | <p>Denies adoption if a device's VLAN matches &lt;VLAN-ID&gt;</p> <ul style="list-style-type: none"> <li>• &lt;VLAN-ID&gt; – Specify the VLAN ID.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                |

## Examples

```
rfs4000-229D58(config-auto-provisioning-policy-test)#deny ap8432 precedence 1 mac 74-67-F7-07-02-35
rfs4000-229D58(config-auto-provisioning-policy-test)#deny ap8432 precedence 2 ip 192.168.13.24 102.168.13.26
rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
default-adoption
deny ap8432 precedence 1 mac 74-67-F7-07-02-35
deny ap8432 precedence 2 ip 192.168.13.24 102.168.13.26
adopt ap8432 precedence 5 profile default-ap8432 rf-domain TechPubs vlan 1
rfs4000-229D588(config-auto-provisioning-policy-test)#
```

## Related Commands

|                                                                                 |
|---------------------------------------------------------------------------------|
| <code>no</code> Removes a deny adoption rule from this Auto Provisioning Policy |
|---------------------------------------------------------------------------------|

### *evaluate-always*

Sets flag to run this auto-provisioning policy every time an access point is adopted. The access point's previous adoption status is not taken into consideration.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
evaluate-always
```

## Parameters

None

## Examples

```
rfs4000-229D58(config-auto-provisioning-policy-test)#evaluate-always
rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
default-adoption
evaluate-always
deny ap8432 precedence 1 mac 74-67-F7-07-02-35
deny ap8432 precedence 2 ip 192.168.13.24 102.168.13.26
adopt ap8432 precedence 5 profile default-ap8432 rf-domain TechPubs vlan 1
rfs4000-229D58(config-auto-provisioning-policy-test)#
```

## Related Commands

|                              |                                                                 |
|------------------------------|-----------------------------------------------------------------|
| <code>no</code> on page 1353 | Disables the running of this policy every time an AP is adopted |
|------------------------------|-----------------------------------------------------------------|

### *redirect*

Adds a rule redirecting device adoption to another controller within the system. Devices seeking adoption are redirected to a specified controller based on the redirection parameters specified.

## Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
redirect [anyap|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|
ap7632|
ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75XX|nx95XX|vx9000|nx96XX]
redirect [anyap|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|
ap7632|
ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75XX|nx95XX|vx9000|Nnx96XX] precedence
<1-10000>
controller [<CONTROLLER-IP>|<CONTROLLER-HOSTNAME>] [any|cdp-match|dhcp-option|fqdn|ip|ipv6|
level|
lldp-match|mac|model-number|pool|serial-number|vlan]
redirect [anyap|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|
ap7632|
ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75XX|nx95XX|vx9000|nx96XX] precedence
<1-10000>
controller [<CONTROLLER-IP>|<CONTROLLER-HOSTNAME>|ipv6] any
redirect [anyap|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|
ap7632|
ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75XX|nx95XX|vx9000|nx96XX] precedence
<1-10000>
controller [<CONTROLLER-IP>|<CONTROLLER-HOSTNAME>|ipv6] [cdp-match <LOCATION-SUBSTRING>|
dhcp-option <DHCP-OPTION>|fqdn <FQDN>|ip [<START-IP> <END-IP>|<IP/MASK>]|ipv6 [<START-IP>
<END-IP>|
<IP/MASK>]|level [1|2]|lldp-match <LLDP-STRING>|mac <START-MAC> {<END-MAC>}]
model-number <MODEL-NUMBER>|pool <1-2>|serial-number <SERIAL-NUMBER>|vlan <VLAN-ID>]
{upgrade}
```

## Parameters

```
redirect [anyap|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|
ap7632|
ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75XX|nx95XX|vx9000|nx96XX] precedence
<1-10000>
controller [<CONTROLLER-IP>|<CONTROLLER-HOSTNAME>|ipv6] any
```

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| redirect                | <p>Adds a redirect adoption rule. The rule applies to the device type selected. Specify the device type and assign a precedence to the rule.</p> <p>The different device types are:<br/>AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533, RFS 4000, NX 5500, NX 75XX, NX 95XX, NX 96XX, and VX 9000.</p> <p><b>Note:</b> 'anyap' is used in auto provisioning policies to create rules that are applicable to any AP regardless of the model type.</p> <p><b>Note:</b> An adoptee controller, such as RFS 4000 can be redirected to another controller (configured to adopt controllers) with a capacity equal to or higher than its own. For more information, see <a href="#">controller</a> on page 918</p> |
| precedence<br><1-10000> | <p>Sets the rule precedence. Rules with lower values get precedence over rules with higher values.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |



|                                                            |                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| controller<br>[<CONTROLLER-IP> <CONTROLLER-HOSTNAME> ipv6] | Configures the controller to which the adopting devices are redirected. Specify the controller's IP address or hostname. <ul style="list-style-type: none"> <li>• &lt;CONTROLLER-IP&gt; - Specifies the controller's IP address</li> <li>• &lt;CONTROLLER-HOSTNAME&gt; - Specifies the controller's hostname</li> <li>• ipv6 - Specify the controller's IPv6 address</li> </ul> |
| any                                                        | Indicates any device. Any device seeking adoption is redirected.                                                                                                                                                                                                                                                                                                                |

```

redirect [anyap|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|
ap7632|
ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75XX|nx95XX|vx9000|nx96XX] precedence
<1-1000>
controller [<CONTROLLER-IP>|<CONTROLLER-HOSTNAME>|ipv6] [cdp-match <LOCATION-SUBSTRING>|
dhcp-option <DHCP-OPTION>|fqdn <FQDN>|ip [<START-IP> <END-IP>|<IP/MASK>]|ipv6 [<START-IP>
<END-IP>|<IP/MASK>]|lldp-match <LLDP-STRING>|mac <START-MAC> {<END-MAC>}|model-number
<MODEL-NUMBER>|pool <1-2>|serial-number <SERIAL-NUMBER>|vlan <VLAN-ID>] {upgrade}

```

|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| redirect                                                   | <p>Adds a redirect adoption rule. The rule applies to the device type selected. Specify the device type and assign a precedence to the rule.</p> <p>The different device types are:<br/>AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533, RFS 4000, NX 5500, NX 75XX, NX 95XX, NX 96XX, and VX 9000.</p> <p><b>Note:</b> 'anyap' is used in auto provisioning policies to create rules that are applicable to any AP regardless of the model type.</p> <p><b>Note:</b> An adoptee controller, such as RFS 4000 can be redirected to another controller (configured to adopt controllers) with a capacity equal to or higher than its own. For more information, see <a href="#">controller</a> on page 918.</p> |
| precedence <1-10000>                                       | Sets the rule precedence. Rules with lower values get precedence over rules with higher values.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| controller<br>[<CONTROLLER-IP> <CONTROLLER-HOSTNAME> ipv6] | <p>Configures the controller to which the adopting devices are redirected. Specify the controller's IP address or hostname.</p> <ul style="list-style-type: none"> <li>• &lt;CONTROLLER-IP&gt; - Specifies the controller's IP address</li> <li>• &lt;CONTROLLER-HOSTNAME&gt; - Specifies the controller's hostname</li> <li>• ipv6 - Specify the controller's IPv6 address</li> </ul> <p>After specifying the rule precedence and the controller, specify the match criteria.</p>                                                                                                                                                                                                                                                                                                                   |
| cdp-match<br><LOCATION-SUBSTRING>                          | <p>Configures the device location to match, based on CDP snoop strings</p> <ul style="list-style-type: none"> <li>• &lt;LOCATION-SUBSTRING&gt; - Specify the location. Devices matching the specified string are redirected.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| dhcp-option <DHCP-OPTION>                                  | <p>Configures the DHCP options to match</p> <p>DHCP options identify the vendor and DHCP client functionalities. This information is used by the client to convey to the DHCP server that the client requires extra information in a DHCP response.</p> <ul style="list-style-type: none"> <li>• &lt;DHCP-OPTION&gt; - Specify the DHCP option value. Devices matching the specified value are redirected.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                |

|                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| fqdn <FQDN>                           | <p>Configures the FQDN to match</p> <p>FQDN is a domain name that specifies its exact location in the DNS hierarchy. It specifies all domain levels, including its top-level domain and the root domain.</p> <ul style="list-style-type: none"> <li>• &lt;FQDN&gt; – Specify the FQDN. Devices matching the specified value are redirected.</li> </ul>                                                                                                                                                                   |
| ip [<START-IP> <END-IP> <IP/MASK>]    | <p>Configures a range of IP addresses and subnet address. Devices having IPv4 addresses within the specified range or are part of the specified subnet are redirected.</p> <ul style="list-style-type: none"> <li>• &lt;START-IP&gt; – Specify the first IPv4 address in the range. <ul style="list-style-type: none"> <li>• &lt;END-IP&gt; – Specify the last IPv4 address in the range.</li> </ul> </li> <li>• &lt;IP/MASK&gt; – Specify the IPv4 subnet and mask to match against the device's IP address.</li> </ul> |
| level[1 2]                            | <p>Configures the routing level</p> <ul style="list-style-type: none"> <li>• level1 – Specifies level 1 as local routing</li> <li>• level2 – Specifies level2 as inter-site routing</li> </ul>                                                                                                                                                                                                                                                                                                                           |
| ipv6 [<START-IP> <END-IP>  <IP/MASK>] | <p>Redirects if a device's IPv6 address matches the specified IP address or is within the specified IP address range</p> <ul style="list-style-type: none"> <li>• &lt;START-IP&gt; – Specify the first IPv6 address in the range. <ul style="list-style-type: none"> <li>• &lt;END-IP&gt; – Specify the last IPv6 address in the range.</li> </ul> </li> <li>• &lt;IP/MASK&gt; – Specify the IPv6 subnet and mask to match against the device's IP address.</li> </ul>                                                   |
| lldp-match <LLDP-STRING>              | <p>Configures the device location to match, based on LLDP snoop string</p> <p>LLDP is a vendor neutral link layer protocol used to advertise a network device's identity, capabilities, and neighbors on a local area network.</p> <ul style="list-style-type: none"> <li>• &lt;LLDP-STRING&gt; – Specify the location. Devices matching the specified string are redirected.</li> </ul>                                                                                                                                 |
| mac <START-MAC> {<END-MAC>}           | <p>Configures a single or a range of MAC addresses. Devices matching the specified values are redirected.</p> <ul style="list-style-type: none"> <li>• &lt;START-MAC&gt; – Specify the first MAC address in the range. Provide only this MAC address to filter a single device.</li> <li>• &lt;END-MAC&gt; – Optional. Specify the last MAC address in the range.</li> </ul>                                                                                                                                             |
| model-number <MODEL-NUMBER>           | <p>Configures the device model number</p> <ul style="list-style-type: none"> <li>• &lt;MODEL-NUMBER&gt; – Specify the model number. Devices matching the specified model number are redirected.</li> </ul>                                                                                                                                                                                                                                                                                                               |
| pool <1-2>                            | <p>Configures the controller pool</p> <ul style="list-style-type: none"> <li>• &lt;1-2&gt; – Configures the pool to which the specified controller belongs to. The default pool value is 1.</li> </ul>                                                                                                                                                                                                                                                                                                                   |
| serial-nuber <SERIAL-NUMBER>          | <p>Configures the device's serial number</p> <ul style="list-style-type: none"> <li>• &lt;SERIAL-NUMBER&gt; – Specify the serial number. Devices matching the specified serial number are redirected.</li> </ul>                                                                                                                                                                                                                                                                                                         |
| vlan <VLAN-ID>                        | <p>Configures the VLAN ID</p> <ul style="list-style-type: none"> <li>• &lt;VLAN-ID&gt; – Specify the VLAN ID. Devices assigned to the specified VLAN ID are redirected.</li> </ul>                                                                                                                                                                                                                                                                                                                                       |
| upgrade                               | <p>Optional. Upgrades APs before redirecting the device for adoption within the system</p>                                                                                                                                                                                                                                                                                                                                                                                                                               |

## Examples

```
rfs4000-229D58(config-auto-provisioning-policy-test)#redirect ap81xx precedence 6
controller 192.168.13.10 ip 192.168.13.11 192.168.13.15
rfs4000-229D58(config-auto-provisioning-policy-test)#redirect ap7532 precedence 7
controller 192.168.13.10 model-number AP-7532-67030-WR
rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 default-adoption
 evaluate-always
 deny ap8432 precedence 1 mac 74-67-F7-07-02-35
 deny ap8432 precedence 2 ip 192.168.13.24 102.168.13.26
 adopt ap8432 precedence 5 profile default-ap8432 rf-domain TechPubs vlan 1
 redirect ap81xx precedence 6 controller 192.168.13.10 ip 192.168.13.11 192.168.13.15
 redirect ap7532 precedence 7 controller 192.168.13.10 model-number AP-7532-67030-WR
rfs4000-229D58(config-auto-provisioning-policy-test)#
```

## Related Commands

|           |                                                            |
|-----------|------------------------------------------------------------|
| <b>no</b> | Removes a redirect rule from this Auto Provisioning Policy |
|-----------|------------------------------------------------------------|

## upgrade

Adds a device upgrade rule to this auto provisioning policy. When applied to a controller, the upgrade rule ensures adopted devices, of the specified type, are upgraded automatically.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
upgrade [anyap|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|
ap7622|ap7632|ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx95xx|vx9000|nx96xx]
upgrade [anyap|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|
ap7622|ap7632|ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx95xx|vx9000|nx96xx]
precedence <1-10000> [any|cdp-match|dhcp-option|fqdn|ip|ipv6|lldp-match|mac|model-number|
serial-number|vlan]
upgrade [anyap|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|
ap7622|ap7632|ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx95xx|vx9000|nx96xx]
precedence <1-10000> [cdp-match <LOCATION-SUBSTRING>|dhcp-option <DHCP-OPTION>|fqdn <FQDN>|
ip [<START-IP> <END-IP>|<IP/MASK>]|ipv6 [<START-IP> <END-IP>|<IP/MASK>]|
lldp-match <LLDP-STRING>|mac <START-MAC> {<END-MAC>}|model-number <MODEL-NUMBER>|
serial-number <SERIAL-NUMBER>|vlan <VLAN-ID>]
```

## Parameters

```
upgrade [anyap|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|
ap7622|ap7632|ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx95xx|vx9000|nx96xx]
precedence <1-10000> any
```

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| upgrade              | <p>Adds a device upgrade rule. The rule applies to the device type selected. Specify the device type and assign a precedence to the rule.</p> <p>The different device types are:<br/> AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533, RFS 4000, NX 5500, NX 75XX, NX 95XX, NX 96XX, and VX 9000.</p> <p><b>Note:</b> Use the 'anyap' option to auto provision any AP regardless of its model type.</p> |
| precedence <1-10000> | Sets the rule precedence. Rules with lower values get precedence over rules with higher values.                                                                                                                                                                                                                                                                                                                                                                                               |
| any                  | Indicates any device. Any device, of the selected type, is upgraded.                                                                                                                                                                                                                                                                                                                                                                                                                          |

```

upgrade [anyap|ap6522|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|
ap7622|ap7632|ap7662|ap81xx|ap8432|ap8533|rfs4000|nx5500|nx75xx|nx95xx|vx9000|nx96xx]
precedence <1-10000> [cdp-match <LOCATION-SUBSTRING>|dhcp-option <DHCP-OPTION>|fqdn <FQDN>|
ip [<START-IP> <END-IP>|<IP/MASK>]|ipv6 [<START-IP> <END-IP>|<IP/MASK>]]
lldp-match <LLDP-STRING>|mac <START-MAC> {<END-MAC>}|model-number <MODEL-NUMBER>|
serial-number <SERIAL-NUMBER>|vlan <VLAN-ID>]

```

|                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| upgrade                            | <p>Adds a device upgrade rule. The rule applies to the device type selected. Specify the device type and assign a precedence to the rule.</p> <p>The different device types are:<br/> AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533, RFS 4000, NX 5500, NX 75XX, NX 95XX, NX 96XX, and VX 9000.</p> <p><b>Note:</b> Use the 'anyap' option to auto provision any AP regardless of its model type.</p> |
| precedence <1-10000>               | Sets the rule precedence. Rules with lower values get precedence over rules with higher values.                                                                                                                                                                                                                                                                                                                                                                                               |
| cdp-match <LOCATION-SUBSTRING>     | <p>Configures the device location to match, based on CDP snoop strings</p> <ul style="list-style-type: none"> <li>• &lt;LOCATION-SUBSTRING&gt; - Specify the location. Devices matching the specified string are upgraded.</li> </ul>                                                                                                                                                                                                                                                         |
| dhcp-option <DHCP-OPTION>          | <p>Configures the DHCP options to match</p> <p>DHCP options identify the vendor and DHCP client functionalities. This information is used by the client to convey to the DHCP server that the client requires extra information in a DHCP response.</p> <ul style="list-style-type: none"> <li>• &lt;DHCP-OPTION&gt; - Specify the DHCP option value. Devices matching the specified value are upgraded.</li> </ul>                                                                           |
| fqdn <FQDN>                        | <p>Configures the FQDN to match.</p> <p>FQDN is a domain name that specifies its exact location in the DNS hierarchy. It specifies all domain levels, including its top-level domain and the root domain.</p> <ul style="list-style-type: none"> <li>• &lt;FQDN&gt; - Specify the FQDN. Devices matching the specified value are upgraded.</li> </ul>                                                                                                                                         |
| ip [<START-IP> <END-IP> <IP/MASK>] | <p>Upgrades if a device's IPv4 address matches the specified IP address or is within the specified IP address range</p> <ul style="list-style-type: none"> <li>• &lt;START-IP&gt; - Specify the first IPv4 address in the range. <ul style="list-style-type: none"> <li>• &lt;END-IP&gt; - Specify the last IPv4 address in the range.</li> </ul> </li> <li>• &lt;IP/MASK&gt; - Specify the IPv4 subnet and mask to match against the device's IP address.</li> </ul>                         |

|                                              |                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ipv6 [<START-IP><br><END-IP>  <IP/<br>MASK>] | Upgrades if a device's IPv6 address matches the specified IP address or is within the specified IP address range <ul style="list-style-type: none"> <li>• &lt;START-IP&gt; – Specify the first IPv6 address in the range.</li> <li>• &lt;END-IP&gt; – Specify the last IPv6 address in the range.</li> <li>• &lt;IP/MASK&gt; – Specify the IPv6 subnet and mask to match against the device's IP address.</li> </ul> |
| lldp-match <LLDP-<br>STRING>                 | Configures the device location to match, based on LLDP snoop strings. LLDP is a vendor neutral link layer protocol used to advertise a network device's identity, capabilities, and neighbors on a local area network. <ul style="list-style-type: none"> <li>• &lt;LLDP-STRING&gt; – Specify the location. Devices matching the specified string are upgraded.</li> </ul>                                           |
| mac <START-MAC><br>{<END-MAC>}               | Configures a single or a range of MAC addresses. Devices matching the specified values are upgraded. <ul style="list-style-type: none"> <li>• &lt;START-MAC&gt; – Specify the first MAC address in the range. Provide only this MAC address to filter a single device.</li> <li>• &lt;END-MAC&gt; – Optional. Specify the last MAC address in the range.</li> </ul>                                                  |
| model-number<br><MODEL-NUMBER>               | Configures the device model number <ul style="list-style-type: none"> <li>• &lt;MODEL-NUMBER&gt; – Specify the model number. Devices matching the specified model number are upgraded.</li> </ul>                                                                                                                                                                                                                    |
| serial-number<br><SERIAL-NUMBER>             | Configures the device's serial number <ul style="list-style-type: none"> <li>• &lt;SERIAL-NUMBER&gt; – Specify the serial number. Device with the specified serial number is upgraded.</li> </ul>                                                                                                                                                                                                                    |
| vlan <VLAN-ID>                               | Configures the VLAN ID <ul style="list-style-type: none"> <li>• &lt;VLAN-ID&gt; – Specify the VLAN ID. Devices assigned to the specified VLAN are upgraded.</li> </ul>                                                                                                                                                                                                                                               |

## Examples

```

rfs4000-229D58(config-auto-provisioning-policy-test1)#upgrade ap8432 precedence 10 any
rfs4000-229D58(config-auto-provisioning-policy-test1)#upgrade ap7522 precedence 11 vlan 1
rfs4000-229D58(config-auto-provisioning-policy-test1)#show context
auto-provisioning-policy test
 default-adoption
 evaluate-always
 deny ap8432 precedence 1 mac 74-67-F7-07-02-35
 deny ap8432 precedence 2 ip 192.168.13.24 102.168.13.26
 adopt ap8432 precedence 5 profile default-ap8432 rf-domain TechPubs vlan 1
 redirect ap81xx precedence 6 controller 192.168.13.10 ip 192.168.13.11 192.168.13.15
 redirect ap7532 precedence 7 controller 192.168.13.10 model-number AP-7532-67030-WR
 upgrade ap8432 precedence 10 any
 upgrade ap7522 precedence 11 vlan 1
rfs4000-229D58(config-auto-provisioning-policy-test1)#

```

## Related Commands

|                                                                      |
|----------------------------------------------------------------------|
| <b>no</b> Removes an upgrade rule from this Auto Provisioning Policy |
|----------------------------------------------------------------------|

*no*

Removes a deny, permit, or redirect rule from the selected auto provisioning policy

## Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
no [adopt|auto-create-rfd-template|default-adoption|deny|evaluate-always|redirect|upgrade]
no adopt precedence <1-10000>
no auto-create-rfd-template
no deny precedence <1-10000>
no evaluate-always
no default-adoption
no redirect precedence <1-10000>
no upgrade precedence <1-10000>
```

## Parameters

```
no <PARAMETERS>
```

|                 |                                                                                      |
|-----------------|--------------------------------------------------------------------------------------|
| no <PARAMETERS> | Removes a deny, permit, or redirect rule from the specified auto provisioning policy |
|-----------------|--------------------------------------------------------------------------------------|

## Examples

The following example shows the auto-provisioning-policy 'test' settings before the 'no' commands are executed:

```
rfs4000-229D58(config-auto-provisioning-policy-test1)#show context
auto-provisioning-policy test
 default-adoption
 evaluate-always
 deny ap8432 precedence 1 mac 74-67-F7-07-02-35
 deny ap8432 precedence 2 ip 192.168.13.24 102.168.13.26
 adopt ap8432 precedence 5 profile default-ap8432 rf-domain TechPubs vlan 1
 redirect ap81xx precedence 6 controller 192.168.13.10 ip 192.168.13.11 192.168.13.15
 redirect ap7532 precedence 7 controller 192.168.13.10 model-number AP-7532-67030-WR
 upgrade ap8432 precedence 10 any
 upgrade ap7522 precedence 11 vlan 1
rfs4000-229D58(config-auto-provisioning-policy-test1)#
rfs4000-229D58(config-auto-provisioning-policy-test)#no default-adoption
rfs4000-229D58(config-auto-provisioning-policy-test)#no deny precedence 1
rfs4000-229D58(config-auto-provisioning-policy-test)#no redirect precedence 6
rfs4000-229D58(config-auto-provisioning-policy-test)#no upgrade precedence 11
```

The following example shows the auto-provisioning-policy 'test' settings after the 'no' commands are executed:

```
rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 deny ap8432 precedence 2 ip 192.168.13.24 102.168.13.26
 adopt ap8432 precedence 5 profile default-ap8432 rf-domain TechPubs vlan 1
 redirect ap7532 precedence 7 controller 192.168.13.10 model-number AP-7532-67030-WR
 upgrade ap8432 precedence 10 any
rfs4000-229D58(config-auto-provisioning-policy-test)#
```

# ASSOCIATION ACL POLICY

## ASSOCIATION-ACL-POLICY

---

This chapter summarizes the association ACL (Access Control List) policy commands in the CLI command structure. An association ACL is a policy-based ACL that either prevents or allows wireless clients from connecting to a controller managed WLAN.

System administrators can use an association ACL to grant or restrict wireless clients access to the WLAN by specifying client MAC addresses or range of MAC addresses to either include or exclude from controller connectivity. Association ACLs are applied to WLANs as an additional access control mechanism.

Use the (config) instance to configure the association ACL policy. To navigate to the association-acl-policy instance, use the following commands:

```
<DEVICE>(config)#association-acl-policy <POLICY-NAME>
nx9500-6C8809(config)#association-acl-policy test
nx9500-6C8809(config-assoc-acl-test)#?
Association ACL Mode commands:
 deny Specify MAC addresses to be denied
 no Negate a command or set its defaults
 permit Specify MAC addresses to be permitted

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-assoc-acl-test)#
```



### Note

If creating an new association ACL policy, provide a name specific to its function. Avoid naming it after a WLAN it may support. The name cannot exceed 32 characters.

---

Before defining an association ACL policy and applying it to a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- The name and configuration of an association ACL policy should meet the requirements of the WLANs it may map to. However, be careful not to name ACLs after specific WLANs, as individual ACL policies can be used by more than one WLAN.
- You cannot apply more than one MAC based ACL to a layer 2 interface. If a MAC ACL is already configured on a layer 2 interface, and a new MAC ACL is applied to the interface, the new ACL replaces the previously configured one.

## Association-acl-policy-commands

The following table summarizes the association ACL policy configuration commands:

Table: Association ACL Policy Configuration Commands

| Command                          | Description                                                    |
|----------------------------------|----------------------------------------------------------------|
| <code>deny</code> on page 1356   | Specifies a range of MAC addresses denied access to the WLAN   |
| <code>permit</code> on page 1357 | Specifies a range of MAC addresses allowed access to the WLAN  |
| <code>no</code> on page 1359     | Removes a deny or permit rule from this association ACL policy |



### Note

For information on common commands (clear, commit, help, revert, service, show, write, and exit), see [COMMON COMMANDS](#) on page 640.



### Note

The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore ( \_ ) character. In other words, the name of a device cannot contain an underscore.

### *deny*

Creates a list of devices denied access to the managed network. Devices are identified by their MAC address. A single MAC address or a range of MAC addresses can be denied access. This command also sets the precedence on how deny rules are applied. Up to a thousand (1000) deny rules can be defined for every association ACL policy. Each rule has a unique sequential precedence value assigned, and are applied to packets on the basis of this precedence value. Lower the precedence of a rule, higher is its priority. This results in the rule with the lowest precedence being applied first. No two rules can have the same precedence. The default precedence is 1, so be careful to prioritize ACLs accordingly as they are added.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
deny <STARTING-MAC> [<ENDING-MAC> |precedence]
deny <STARTING-MAC> precedence <1-1000>
deny <STARTING-MAC> <ENDING-MAC> precedence <1-1000>
```

#### Parameters

```
deny <STARTING-MAC> precedence <1-1000>
```



|                     |                                                                                                                                                                                                                   |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| deny                | Adds a single device or a set of devices to the deny list                                                                                                                                                         |
| <STARTING-MAC>      | To add a single device, enter its MAC address in the <STARTING-MAC> parameter.                                                                                                                                    |
| precedence <1-1000> | Sets a precedence value for this rule. Rules are applied in an increasing order of their precedence. <ul style="list-style-type: none"> <li>&lt;1-1000&gt; - Specify a precedence value from 1 - 1000.</li> </ul> |

```
deny <STARTING-MAC> <ENDING-MAC> precedence <1-1000>
```

|                     |                                                                                                                                                                                         |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| deny                | Adds a single device or a set of devices to the deny list. To add a set of devices, provide the range of MAC addresses.                                                                 |
| <STARTING-MAC>      | Specify the first MAC address in the range.                                                                                                                                             |
| <ENDING-MAC>        | Specify the last MAC address in the range.                                                                                                                                              |
| precedence <1-1000> | Sets a precedence rule. Rules are applied in an increasing order of their precedence. <ul style="list-style-type: none"> <li>&lt;1-1000&gt; - Specify a value from 1 - 1000.</li> </ul> |

### Usage Guidelines

Every rule has a unique sequential precedence value. You cannot add two rules with the same precedence. Rules are checked in an increasing order of precedence. That means, the rule with precedence 1 is checked first, then the rule with precedence 2 and so on.

### Examples

```
nx9500-6C8809(config-assoc-acl-test)#deny 11-22-33-44-55-01 11-22-33-44-55-FF precedence
150
nx9500-6C8809(config-assoc-acl-test)#deny 11-22-33-44-56-01 precedence 160
nx9500-6C8809(config-assoc-acl-test)#show context
association-acl-policy test
 deny 11-22-33-44-55-01 11-22-33-44-55-FF precedence 150
 deny 11-22-33-44-56-01 precedence 160
nx9500-6C8809(config-assoc-acl-test)#
```

### Related Commands

|    |                                                      |
|----|------------------------------------------------------|
| no | Removes a deny rule from this Association ACL Policy |
|----|------------------------------------------------------|

### *permit*

Creates a list of devices allowed access to the managed network. Devices are permitted access based on their MAC address. A single MAC address or a range of MAC addresses can be specified. This command also sets the precedence on how permit list rules are applied. Up to a thousand (1000) permit rules can be defined for every association ACL policy. Each rule has a unique sequential precedence value assigned, and are applied to packets on the basis of this precedence value. Lower the precedence of a rule, higher is its priority. This results in the rule with the lowest precedence being applied first. No two rules can have the same precedence. The default precedence is 1, so be careful to prioritize ACLs accordingly as they are added.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533

- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
permit <STARTING-MAC> [<ENDING-MAC> | precedence]
permit <STARTING-MAC> precedence <1-1000>
permit <STARTING-MAC> <ENDING-MAC> precedence <1-1000>
```

### Parameters

```
permit <STARTING-MAC> precedence <1-1000>
```

|                     |                                                                                                                                                                                                      |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| permit              | Adds a single device or a set of devices to the permit list                                                                                                                                          |
| <STARTING-MAC>      | To add a single device, enter its MAC address in the <STARTING-MAC> parameter.                                                                                                                       |
| precedence <1-1000> | Specifies a rule precedence. Rules are applied in an increasing order of their precedence value. <ul style="list-style-type: none"> <li>• &lt;1-1000&gt; – Specify a value from 1 - 1000.</li> </ul> |

```
permit <STARTING-MAC> <ENDING-MAC> precedence <1-1000>
```

|                     |                                                                                                                                                                                                      |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| permit              | Adds a single device or a set of devices to the permit list To add a set of devices, provide the MAC address range.                                                                                  |
| <STARTING-MAC>      | Specify the first MAC address of the range.                                                                                                                                                          |
| <ENDING-MAC>        | Specify the last MAC address of the range.                                                                                                                                                           |
| precedence <1-1000> | Specifies a rule precedence. Rules are applied in an increasing order of their precedence value. <ul style="list-style-type: none"> <li>• &lt;1-1000&gt; – Specify a value from 1 - 1000.</li> </ul> |

### Usage Guidelines

Every rule has a unique sequential precedence value. You cannot add two rules with the same precedence. Rules are checked in an increasing order of precedence. That means, the rule with precedence 1 is checked first, then the rule with precedence 2 and so on.

### Examples

```
nx9500-6C8809(config-assoc-acl-test)# permit 11-22-33-44-66-01 11-22-33-44-66-FF
precedence 170
nx9500-6C8809(config-assoc-acl-test)# permit 11-22-33-44-67-01 precedence 180
nx9500-6C8809(config-assoc-acl-test)#show context
association-acl-policy test
deny 11-22-33-44-55-01 11-22-33-44-55-FF precedence 150
deny 11-22-33-44-56-01 precedence 160
permit 11-22-33-44-66-01 11-22-33-44-66-FF precedence 170
permit 11-22-33-44-67-01 precedence 180
nx9500-6C8809(config-assoc-acl-test)#
```

### Related Commands

|    |                                                        |
|----|--------------------------------------------------------|
| no | Removes a permit rule from this Association ACL Policy |
|----|--------------------------------------------------------|

no

Removes a deny or permit rule from this Association ACL Policy

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
no [deny|permit]
no deny <STARTING-MAC> precedence <1-1000>
no deny <STARTING-MAC> <ENDING-MAC> precedence <1-1000>
no permit <STARTING-MAC> precedence <1-1000>
no permit <STARTING-MAC> <ENDING-MAC> precedence <1-1000>
```

#### Parameters

no <PARAMETERS>

|                 |                                                                |
|-----------------|----------------------------------------------------------------|
| no <PARAMETERS> | Removes a deny or permit rule from this association ACL policy |
|-----------------|----------------------------------------------------------------|

#### Examples

The following example shows the association ACL policy 'test' settings before the 'no' commands is executed:

```
nx9500-6C8809(config-assoc-acl-test)#show context
association-acl-policy test
 deny 11-22-33-44-55-01 11-22-33-44-55-FF precedence 150
 deny 11-22-33-44-56-01 precedence 160
 permit 11-22-33-44-66-01 11-22-33-44-66-FF precedence 170
 permit 11-22-33-44-67-01 precedence 180
nx9500-6C8809(config-assoc-acl-test)#
nx9500-6C8809(config-assoc-acl-test)#no deny 11-22-33-44-56-01 11-22-33-44-56-FF
precedence 150
```

The following example shows the association ACL policy 'test' settings after the 'no' commands is executed:

```
nx9500-6C8809(config-assoc-acl-test)#show context
association-acl-policy test
 deny 11-22-33-44-56-01 precedence 160
 permit 11-22-33-44-66-01 11-22-33-44-66-FF precedence 170
 permit 11-22-33-44-67-01 precedence 180
nx9500-6C8809(config-assoc-acl-test)#
```

#### Related Commands

|        |                                                      |
|--------|------------------------------------------------------|
| deny   | Adds a device or a set of devices to the deny list   |
| permit | Adds a device or a set of devices to the permit list |

# ACCESS LIST

## ACCESS-LIST

---

This chapter summarizes IP and MAC access list commands in the CLI command structure.

Access lists control access to the managed network using a set of rules also known as ACEs (Access Control Entries). Each rule specifies an action taken when a packet matches that rule. If the action is deny, the packet is dropped. If the action is permit, the packet is allowed. A set of deny and/or permit rules based on IP (IPv4 and IPv6) addresses constitutes a IP ACL (Access Control List). Similarly, a set of deny and/or permit rules based on MAC addresses constitutes a MAC ACL.

Within a managed network, IP ACLs are used as firewalls to filter packets and also mark packets. IP based firewall rules are specific to the source and destination IP addresses and have unique precedence orders assigned. Both IP and non-IP traffic on the same layer 2 interface can be filtered by applying an IP ACL. With either IPv4 or IPv6, create access rules for traffic entering a controller, service platform, or access point interface, because if you are going to deny specific types of packets, it's recommended you do it before the controller, service platform, or access point spends time processing them, since access rules are given priority over other types of firewall rules.

MAC ACLs are firewalls that filter or mark packets based on the MAC address which they arrive, as opposed to filtering packets on layer 2 ports. Optionally filter layer 2 traffic on a physical layer 2 interface using MAC addresses. A MAC firewall rule uses source and destination MAC addresses for matching operations, where the result is a typical allow, deny or mark designation to controller managed packet traffic.

Once defined, an IP and/or MAC ACL (consisting of a set of firewall rules) must be applied to an interface to be a functional filtering tool.

Firewall supported devices (access points, wireless controllers, and service platforms) process firewall rules (within an IP/MAC ACL) sequentially, in ascending order of their precedence value. When a packet matches a rule, the firewall applies the action specified in the rule to determine whether the traffic is allowed or denied. Once a match is made, the firewall does not process subsequent rules in the ACL.

The WiNG software enables the configuration of IP SNMP ACLs. These ACLs control access by combining IP ACLs with SNMP server community strings.

The following ACLs are supported:

- [ip-access-list](#) on page 1363
- [ipv6-access-list](#) on page 1403
- [mac-access-list](#) on page 1389
- [ip-snmp-access-list](#) on page 1415
- [ex3500-ext-access-list](#) on page 1417
- [ex3500-std-access-list](#) on page 1424

Use IP and MAC commands under the global configuration to create an access list.

- When the access list is applied on an Ethernet port, it becomes a port ACL

- When the access list is applied on a VLAN interface, it becomes a router ACL

Use the (config) instance to configure a new ACL or modify an existing ACL. To navigate to the (config-access-list) instance, use the following commands:

```
<DEVICE>(config)#ip access-list <IP-ACCESS-LIST-NAME>
<DEVICE>(config)#mac access-list <MAC-ACCESS-LIST-NAME>
<DEVICE>(config)#ipv6 access-list <IPv6-ACCESS-LIST-NAME>
<DEVICE>(config)#ip snmp-access-list <SNMP-ACCESS-LIST-NAME>
<DEVICE>(config)#ex3500-ext-access-list <EX3500-EXT-ACCESS-LIST-NAME>
<DEVICE>(config)#ex3500-std-access-list <EX3500-STD-ACCESS-LIST-NAME>
```



#### Note

If creating a new ACL policy, provide a name that uniquely identifies its purpose. The name cannot exceed 32 characters.

### IPv4 Access List

```
nx9500-6C8809(config)#ip access-list IPv4ACL
nx9500-6C8809(config-ip-acl-IPv4ACL)#?
ACL Configuration commands:
 deny Specify packets to reject
 disable Disable rule if not needed
 insert Insert this rule (instead of overwriting a existing rule)
 no Negate a command or set its defaults
 permit Specify packets to forward

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-ip-acl-IPv4ACL)#
```

### IPv6 Access List

```
nx9500-6C8809(config)#ipv6 access-list IPv6ACL
nx9500-6C8809(config-ipv6-acl-IPv6ACL)#?
IPv6 Access Control Mode commands:
 deny Specify packets to reject
 no Negate a command or set its defaults
 permit Specify packets to forward

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-ipv6-acl-IPv6ACL)#
```

## MAC Access List

```
nx9500-6C8809(config)#mac access-list MACACL
nx9500-6C8809(config-mac-acl-MACACL)#?
MAC Extended ACL Configuration commands:
 deny Specify packets to reject
 disable Disable rule if not needed
 ex3500 Ex3500 device
 insert Insert this rule (instead of overwriting a existing rule)
 no Negate a command or set its defaults
 permit Specify packets to forward

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-mac-acl-MACACL)#
```

## SNMP Access List

```
nx9500-6C8809(config)#ip snmp-access-list SNMPACL
nx9500-6C8809(config-ip-snmp-acl-SNMPACL)#?
SNMP ACL Configuration commands:
 deny Specify packets to reject
 no Negate a command or set its defaults
 permit Specify packets to forward

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-ip-snmp-acl-SNMPACL)#
```

The WiNG NOC controller also has the capabilities of adopting and managing EX3500 series switch. These switches are Gigabit Ethernet layer 2 switches with either 24 or 48 10/100/1000-BASE-T ports, and four SFP (Small Form Factor Pluggable) transceiver slots for fiber connectivity. Once adopted to the NOC, various ACLs specifically defined for a EX3500 switch can be used to either prevent or allow specific clients from using it.

The following EX3500 ACLs are supported:

- [EX3500 Extended Access List](#).
- [EX3500 Standard Access List](#).

- **EX3500 (MAC ACL)**. This configures a EX3500 deny or permit rule in a MAC ACL.



#### Note

The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore ( \_ ) character. In other words, the name of a device cannot contain an underscore.

## ip-access-list

The following table summarizes IP Access List configuration commands.

Table: IP-Access-List-Config Commands

| Command                                | Description                                                                                                                                                           |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>deny (ipv4-acl)</b> on page 1363    | Creates a deny access rule or modifies an existing rule. A deny access rule rejects packets from specified address(es) and/or destined for specified address(es).     |
| <b>disable (ipv4-acl)</b> on page 1374 | Disables an existing deny or permit rule without removing it from the ACL                                                                                             |
| <b>insert (ipv4-acl)</b> on page 1376  | Inserts a rule in an IP ACL without overwriting or replacing an existing rule having the same precedence                                                              |
| <b>permit (ipv4-acl)</b> on page 1378  | Creates a permit access rule or modifies an existing rule. A permit access rule accepts packets from specified address(es) and/or destined for specified address(es). |
| <b>no (ipv4-acl)</b> on page 1388      | Removes a deny and/or a permit access rule from a IP ACL                                                                                                              |



#### Note

For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see **COMMON COMMANDS** on page 640.

### *deny (ipv4-acl)*

Creates a deny rule that rejects packets received from a specified source IP and/or addressed to a specified destination IP. You can also use this command to modify an existing deny rule.



#### Note

Use a decimal value representation to implement a *permit/deny* designation for a packet. The command set for IP ACLs provides the hexadecimal values for each listed EtherType. Use the decimal equivalent of the EtherType listed for any other EtherType.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
deny [<NETWORK-SERVICE-ALIAS-NAME>|dns-name|icmp|ip|proto|tcp|udp]
deny <NETWORK-SERVICE-ALIAS-NAME> [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|
any|from-vlan <VLAN-ID>|host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|any|host <DEST-HOST-IP>|
<NETWORK-GROUP-ALIAS-NAME>] (log,mark [8021p <0-7>|dscp <0-63>],
rule-precedence <1-5000>) {(rule-description <LINE>)}
deny dns-name [contains|exact|suffix]
deny dns-name [contains|exact|suffix] <WORD> (log,rule-precedence <1-5000>)
{(rule-description <LINE>)}
deny icmp [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|
host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|host <DEST-HOST-IP>]
(<ICMP-TYPE> <ICMP-CODE>,log,rule-precedence <1-5000>) {(rule-description <LINE>)}
deny ip [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|
host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|host <DEST-HOST-IP>]
(log,rule-precedence <1-5000>) {(rule-description <LINE>)}
deny proto [<PROTOCOL-NUMBER>|<PROTOCOL-NAME>|eigrp|gre|igmp|igp|ospf|vrrp]
[<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|host <SOURCE-HOST-
IP>]
[<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|host <DEST-HOST-IP>] (log,rule-precedence
<1-5000>)
{(rule-description <LINE>)}
deny [tcp|udp] [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|
host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|eq <SOURCE-PORT>|
host <DEST-HOST-IP>|range <START-PORT> <END-PORT>] [eq [<1-65535>|<SERVICE-NAME>|bgp|dns|
ftp]
ftp-data|gopher|https|ldap|nntp|ntp|pop3|sip|smtp|ssh|telnet|tftp|www]|range <START-PORT>
<END-PORT>]
(log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

## Parameters

```
deny <NETWORK-SERVICE-ALIAS-NAME> [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|
from-vlan <VLAN-ID>|host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|any|host <DEST-HOST-IP>|
<NETWORK-GROUP-ALIAS-NAME>]
(log,mark [8021p <0-7>|dscp <0-63>],rule-precedence <1-5000>) {(rule-description <LINE>)}
```

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <NETWORK-SERVICE-ALIAS-NAME> | <p>Applies this deny rule to packets based on service protocols and ports specified in the network-service alias</p> <ul style="list-style-type: none"> <li>&lt;NETWORK-SERVICE-ALIAS-NAME&gt; - Specify the network-service alias name (should be existing and configured).</li> </ul> <p>A network-service alias defines service protocols and ports to match. When used with an ACL, the network-service alias defines the service-specific components of the ACL deny rule.</p> <p><b>Note:</b> For more information on configuring network-service alias, see <a href="#">alias</a>.</p>                                                 |
| <SOURCE-IP/MASK>             | <p>Specifies the source IP address and mask (A.B.C.D/M) to match. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified network are dropped.</p>                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <NETWORK-GROUP-ALIAS-NAME>   | <p>Applies a network-group alias to identify the source IP addresses. Packets, matching the service protocols and ports specified in the network-service alias, received from the addresses identified by the network-group alias are dropped.</p> <ul style="list-style-type: none"> <li>&lt;NETWORK-GROUP-ALIAS-NAME&gt; - Specify the network-group alias name (should be existing and configured).</li> </ul> <p>A network-group alias defines a single or a range of addresses of devices, hosts, and networks. When used with an ACL, the network-group alias defines the network-specific component of the ACL rule (permit/deny).</p> |
| any                          | <p>Specifies the source as any source IP address. Packets, matching the service protocols and ports specified in the network-service alias, received from any source are dropped.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                         |



|                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| from-vlan <VLAN-ID>                              | <p>Specifies a single VLAN or a range of VLANs as the match criteria. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified VLAN(s) are dropped.</p> <ul style="list-style-type: none"> <li>• &lt;VLAN-ID&gt; – Specify the VLAN ID. To configure a range of VLANs, enter the start and end VLAN IDs separated by a hyphen (for example, 12-20).</li> </ul> <p><b>Note:</b> Use this option with WLANs and port ACLs.</p>                                                                                                                                                                                                             |
| host <SOURCE-HOST-IP>                            | <p>Identifies a specific host (as the source to match) by its IP address. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified host are dropped.</p> <ul style="list-style-type: none"> <li>• &lt;SOURCE-HOST-IP&gt; – Specify the source host's exact IP address in the A.B.C.D format.</li> </ul>                                                                                                                                                                                                                                                                                                                                  |
| <DEST-IP/MASK>                                   | <p>Specifies the destination IP address and mask (A.B.C.D/M) to match. Packets, matching the service protocols and ports specified in the network-service alias, addressed to the specified network are dropped.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| any                                              | <p>Specifies the destination as any destination IP address. Packets, matching the service protocols and ports specified in the network-service alias, addressed to any destination are dropped.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| host <DEST-HOST-IP>                              | <p>Identifies a specific host (as the destination to match) by its IP address. Packets, matching the service protocols and ports specified in the network-service alias, addressed to the specified host are dropped.</p> <ul style="list-style-type: none"> <li>• &lt;DEST-HOST-IP&gt; – Specify the destination host's exact IP address in the A.B.C.D format.</li> </ul>                                                                                                                                                                                                                                                                                                                           |
| <NETWORK-GROUP-ALIAS-NAME>                       | <p>Applies a network-group alias to identify the destination IP addresses. Packets, matching the service protocols and ports specified in the network-service alias, destined for the addresses identified by the network-group alias are dropped.</p> <ul style="list-style-type: none"> <li>• &lt;NETWORK-GROUP-ALIAS-NAME&gt; – Specify the network-group alias name (should be existing and configured).</li> </ul>                                                                                                                                                                                                                                                                               |
| log                                              | <p>Logs all deny events matching this entry. If a source and/or destination IP address is matched (i.e. if any specified type of packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| mark [8021p <0-7>  dscp <0-63>]                  | <p>Specifies packets to mark</p> <ul style="list-style-type: none"> <li>• 8021p &lt;0-7&gt; – Marks packets by modifying 802.1p VLAN user priority</li> <li>• dscp &lt;0-63&gt; – Marks packets by modifying DSCP TOS bits in the header</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| rule-precedence <1-5000> rule-description <LINE> | <p>The following keywords are recursive and common to all of the above parameters:</p> <ul style="list-style-type: none"> <li>• rule-precedence – Assigns a precedence for this deny rule <ul style="list-style-type: none"> <li>• &lt;1-5000&gt; – Specify a value from 1 - 5000.</li> </ul> </li> </ul> <p><b>Note:</b> Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.</p> <ul style="list-style-type: none"> <li>• rule-description – Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).</li> </ul> |

```
deny dns-name [contains|exact|suffix] <WORD> (log,rule-precedence <1-5000>)
{(rule-description <LINE>)}
```

|                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dns-name                                            | Applies this deny rule to packets based on dns-names specified in the network-service                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| contains                                            | Matches any hostname which has this DNS label. (for example, *.test.*)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| exact                                               | Matches an exact hostname as specified in the network-service                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| syffix                                              | Matches any hostname as suffix (for example, *.test)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <WORD>                                              | Identifies a specific host (as the source to match) by its domain name. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified host are dropped.                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| log                                                 | Logs all deny events matching this dns entry. If a dns-name is matched an event is logged.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| rule-precedence <1-5000><br>rule-description <LINE> | <p>The following keywords are recursive and common to all of the above parameters:</p> <ul style="list-style-type: none"> <li>rule-precedence – Assigns a precedence for this deny rule <ul style="list-style-type: none"> <li>&lt;1-5000&gt; – Specify a value from 1 - 5000.</li> </ul> <p><b>Note:</b> Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.</p> </li> <li>rule-description – Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).</li> </ul> |

```
deny icmp [<SOURCE-IP/MASK>|<NETWORK-GROUP-NAME>|any|from-vlan <VLAN-ID>|
host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-NAME>|any|host <DEST-HOST-IP>]
(<ICMP-TYPE> <ICMP-CODE>,log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| icmp                       | Applies this deny rule to ICMP (Internet Control Message Protocol) packets only                                                                                                                                                                                                                                                                                                                                |
| <SOURCE-IP/MASK>           | Specifies the source IP address and mask (A.B.C.D/M) to match. ICMP packets received from the specified sources are dropped.                                                                                                                                                                                                                                                                                   |
| <NETWORK-GROUP-ALIAS-NAME> | <p>Applies a network-group alias to identify the source IP addresses. ICMP packets received from the addresses identified by the network-group alias are dropped.</p> <ul style="list-style-type: none"> <li>&lt;NETWORK-GROUP-ALIAS-NAME&gt; – Specify the network-group alias name (should be existing and configured).</li> </ul>                                                                           |
| any                        | Specifies the source as any IP address. ICMP packets received from any source are dropped.                                                                                                                                                                                                                                                                                                                     |
| from-vlan <VLAN-ID>        | <p>Specifies a single VLAN or a range of VLANs as the match criteria. ICMP packets received from the VLANs identified here are dropped.</p> <ul style="list-style-type: none"> <li>&lt;VLAN-ID&gt; – Specify the VLAN ID. To configure a range of VLANs, enter the start and end VLAN IDs separated by a hyphen (for example, 12-20).</li> </ul> <p><b>Note:</b> Use this option with WLANs and port ACLs.</p> |
| host <SOURCE-HOST-IP>      | <p>Identifies a specific host (as the source to match) by its IP address. ICMP packets received from the specified host are dropped.</p> <ul style="list-style-type: none"> <li>&lt;SOURCE-HOST-IP&gt; – Specify the source host's exact IP address in the A.B.C.D format.</li> </ul>                                                                                                                          |
| <DEST-IP/MASK>             | Specifies the destination IP address and mask (A.B.C.D/M) to match. ICMP packets addressed to specified destinations are dropped.                                                                                                                                                                                                                                                                              |

|                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <NETWORK-GROUP-ALIAS-NAME>                       | <p>Applies a network-group alias to identify the destination IP addresses. ICMP packets destined for addresses identified by the network-group alias are dropped.</p> <ul style="list-style-type: none"> <li>• &lt;NETWORK-GROUP-ALIAS-NAME&gt; – Specify the network-group alias name (should be existing and configured).</li> </ul>                                                                                                                                                                                                                                                                                                                       |
| any                                              | Specifies the destination as any IP address. ICMP packets addressed to any destination are dropped.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| host <DEST-HOST-IP>                              | <p>Identifies a specific host (as the destination to match) by its IP address. ICMP packets addressed to the specified host are dropped.</p> <ul style="list-style-type: none"> <li>• &lt;DEST-HOST-IP&gt; – Specify the destination host's exact IP address in the A.B.C.D format.</li> </ul>                                                                                                                                                                                                                                                                                                                                                               |
| <ICMP-TYPE>                                      | <p>Defines the ICMP packet type<br/>For example, an ICMP type 0 indicates it is an ECHO REPLY, and type 8 indicates it is an ECHO.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <ICMP-CODE>                                      | <p>Defines the ICMP message type<br/>For example, an ICMP code 3 indicates "Destination Unreachable", code 1 indicates "Host Unreachable", and code 3 indicates "Port Unreachable."</p> <p><b>Note:</b> After specifying the source and destination IP address(es), the ICMP message type, and the ICMP code, specify the action taken in case of a match.</p>                                                                                                                                                                                                                                                                                               |
| log                                              | Logs all deny events matching this entry. If a source and/or destination IP address is matched (i.e. a ICMP packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged.                                                                                                                                                                                                                                                                                                                                                                                                                               |
| rule-precedence <1-5000> rule-description <LINE> | <p>The following keywords are recursive and common to all of the above parameters:</p> <ul style="list-style-type: none"> <li>• rule-precedence – Assigns a precedence for this deny rule <ul style="list-style-type: none"> <li>• &lt;1-5000&gt; – Specify a value from 1 - 5000.</li> </ul> <p><b>Note:</b> Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.</p> </li> <li>• rule-description – Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).</li> </ul> |

```
deny ip [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|
host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|host <DEST-HOST-IP>]
(log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

|                            |                                                                                                                                                                                                                                                                                                                                      |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip                         | Applies this deny rule to IP packets only                                                                                                                                                                                                                                                                                            |
| <SOURCE-IP/MASK>           | Specifies the source IP address and mask (A.B.C.D/M) to match. IP packets received from the specified networks are dropped.                                                                                                                                                                                                          |
| <NETWORK-GROUP-ALIAS-NAME> | <p>Applies a network-group alias to identify the source IP addresses. IP packets received from the addresses identified by the network-group alias are dropped.</p> <ul style="list-style-type: none"> <li>• &lt;NETWORK-GROUP-ALIAS-NAME&gt; – Specify the network-group alias name (should be existing and configured).</li> </ul> |
| any                        | Specifies the source as any IP address. IP packets received from any source are dropped.                                                                                                                                                                                                                                             |

|                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| from-vlan <VLAN-ID>                              | <p>Specifies a single VLAN or a range of VLANs as the match criteria. IP packets received from the specified VLANs are dropped.</p> <ul style="list-style-type: none"> <li>• &lt;VLAN-ID&gt; – Specify the VLAN ID. To configure a range of VLAN IDs, enter the start and end VLAN IDs separated by a hyphen (for example, 12-20).</li> </ul> <p><b>Note:</b> Use this option with WLANs and port ACLs.</p>                                                                                                                                                                            |
| host <SOURCE-HOST-IP>                            | <p>Identifies a specific host (as the source to match) by its IP address. IP packets received from the specified host are dropped.</p> <ul style="list-style-type: none"> <li>• &lt;SOURCE-HOST-IP&gt; – Specify the source host’s exact IP address in the A.B.C.D format.</li> </ul>                                                                                                                                                                                                                                                                                                  |
| <DEST-IP/MASK>                                   | <p>Specifies the destination IP address and mask (A.B.C.D/M) to match. IP packets addressed to the specified networks are dropped.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| any                                              | <p>Specifies the destination as any IP address. IP packets addressed to any destination are dropped.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| host <DEST-HOST-IP>                              | <p>Identifies a specific host (as the destination to match) by its IP address. IP packets addressed to the specified host are dropped.</p> <ul style="list-style-type: none"> <li>• &lt;DEST-HOST-IP&gt; – Specify the destination host’s exact IP address in the A.B.C.D format.</li> </ul>                                                                                                                                                                                                                                                                                           |
| <NETWORK-GROUP-ALIAS-NAME>                       | <p>Applies a network-group alias to identify the source IP addresses. IP packets destined for addresses identified by the network-group alias are dropped.</p> <ul style="list-style-type: none"> <li>• &lt;NETWORK-GROUP-ALIAS-NAME&gt; – Specify the network-group alias name (should be existing and configured).</li> </ul>                                                                                                                                                                                                                                                        |
| log                                              | <p>Logs all deny events matching this entry. If a source and/or destination IP address is matched (i.e. a IP packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged.</p>                                                                                                                                                                                                                                                                                                                                                    |
| rule-precedence <1-5000> rule-description <LINE> | <p>The following keywords are recursive and common to all of the above parameters:</p> <ul style="list-style-type: none"> <li>• &lt;1-5000&gt; – Specify a value from 1 - 5000.</li> </ul> <p><b>Note:</b> Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.</p> <ul style="list-style-type: none"> <li>• rule-description – Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).</li> </ul> |

```
deny proto [<PROTOCOL-NUMBER>|<PROTOCOL-NAME>|eigrp|gre|igmp|igp|ospf|vrrp]
[<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|
host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|
host <DEST-HOST-IP>] (log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

|                   |                                                                                                                                                                                                            |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| proto             | <p>Configures the ACL for additional protocols<br/>Additional protocols (other than IP, ICMP, TCP, and UDP) must be configured using this parameter</p>                                                    |
| <PROTOCOL-NUMBER> | <p>Filters protocols using their IANA (Internet Assigned Numbers Authority) protocol number</p> <ul style="list-style-type: none"> <li>• &lt;PROTOCOL-NUMBER&gt; – Specify the protocol number.</li> </ul> |
| <PROTOCOL-NAME>   | <p>Filters protocols using their IANA protocol name</p> <ul style="list-style-type: none"> <li>• &lt;PROTOCOL-NAME&gt; – Specify the protocol name.</li> </ul>                                             |

|                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| eigrp                              | Identifies the EIGRP (Enhanced Internet Gateway Routing Protocol) protocol (number 88) EIGRP enables routers to maintain copies of neighbors' routing tables. Routers use this information to determine the fastest route to a destination. When a router fails to find a route in its stored route tables, it sends a query to neighbors who in turn query their neighbors till a route is found. EIGRP also enables routers to inform neighbors of changes in their routing tables.                                                |
| gre                                | Identifies the GRE (General Routing Encapsulation) protocol (number 47) GRE is a tunneling protocol that enables transportation of protocols (IP, IPX, DEC net, etc.) over an IP network. GRE encapsulates the packet at the source and removes the encapsulation at the destination.                                                                                                                                                                                                                                                |
| igmp                               | Identifies the IGMP (Internet Group Management Protocol) protocol (number 2) IGMP establishes and maintains multicast group memberships to interested members. Multicasting allows a networked computer to send content to multiple computers who have registered to receive the content. IGMP snooping is for listening to IGMP traffic between an IGMP host and routers in the network to maintain a map of the links that require multicast streams. Multicast traffic is filtered out for those links which do not require them. |
| igp                                | Identifies any private internal gateway (primarily used by CISCO for their IGRP) (number 9) IGP enables exchange of information between hosts and routers within a managed network. The most commonly used IGP (interior gateway protocol) protocols are: RIP (Routing Information Protocol) and OSPF (Open Shortest Path First).                                                                                                                                                                                                    |
| ospf                               | Identifies the OSPF protocol (number 89) OSPF is a link-state IGP. OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets.                                                                                           |
| vrrp                               | Identifies the VRRP (Virtual Router Redundancy Protocol) protocol (number 112) VRRP allows a pool of routers to be advertised as a single virtual router. This virtual router is configured by hosts as their default gateway. VRRP elects a master router, from this pool, and assigns it a virtual IP address. The master router routes and forwards packets to hosts on the same subnet. When the master router fails, one of the backup routers is elected as the master and its IP address is mapped to the virtual IP address. |
| <SOURCE-IP/<br>MASK>               | Specifies the source IP address and mask (A.B.C.D/M) to match. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the specified sources are dropped.                                                                                                                                                                                                                                                                                                                                                                       |
| <NETWORK-<br>GROUP-ALIAS-<br>NAME> | Applies a network-group alias to identify the source IP addresses. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the sources defined in the network-group alias are dropped. <ul style="list-style-type: none"> <li>• &lt;NETWORK-GROUP-ALIAS-NAME&gt; - Specify the network-group alias name (should be existing and configured).</li> </ul>                                                                                                                                                                         |
| any                                | Specifies the source as any IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from any source are dropped.                                                                                                                                                                                                                                                                                                                                                                                                         |
| from-vlan<br><VLAN-ID>             | Specifies a single VLAN or a range of VLANs as the match criteria. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the VLANs identified here are dropped. <ul style="list-style-type: none"> <li>• &lt;VLAN-ID&gt; - Specify the VLAN ID. A range of VLANs is represented by the start and end VLAN IDs separated by a hyphen (for example, 12-20).</li> </ul> <p><b>Note:</b> Use this option with WLANs and port ACLs.</p>                                                                                            |

|                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| host <SOURCE-HOST-IP>                            | Identifies a specific host (as the source to match) by its IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the specified host are dropped. <ul style="list-style-type: none"> <li>&lt;SOURCE-HOST-IP&gt; – Specify the source host’s exact IP address in the A.B.C.D format.</li> </ul>                                                                                                                                                                                                                                                                                                                                |
| <DEST-IP/MASK>                                   | Specifies the destination IP address and mask (A.B.C.D/M) to match. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to the specified destinations are dropped.                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| any                                              | Specifies the destination as any IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to any destination are dropped.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| host <DEST-HOST-IP>                              | Identifies a specific host (as the destination to match) by its IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addresses to the specified host are dropped. <ul style="list-style-type: none"> <li>&lt;SOURCE-HOST-IP&gt; – Specify the destination host’s exact IP address in the A.B.C.D format.</li> </ul>                                                                                                                                                                                                                                                                                                                       |
| <NETWORK-GROUP-ALIAS-NAME>                       | Applies a network-group alias to identify the destination IP addresses. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to the destinations identified in the network-group alias are dropped. <ul style="list-style-type: none"> <li>&lt;NETWORK-ALIAS-NAME&gt; – Specify the network-group alias name (should be existing and configured).</li> </ul> <p><b>Note:</b> After specifying the source and destination IP address(es), specify the action taken in case of a match.</p>                                                                                                                                                   |
| log                                              | Logs all deny events matching this entry. If a source and/or destination IP address is matched (i.e. a packet (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) is received from a specified IP address and/or is destined for a specified IP address), an event is logged.                                                                                                                                                                                                                                                                                                                                                                                |
| rule-precedence <1-5000> rule-description <LINE> | The following keywords are recursive and common to all of the above parameters: <ul style="list-style-type: none"> <li>rule-precedence – Assigns a precedence for this deny rule <ul style="list-style-type: none"> <li>&lt;1-5000&gt; – Specify a value from 1 - 5000.</li> </ul> <p><b>Note:</b> Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.</p> </li> <li>rule-description – Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).</li> </ul> |

```
deny [tcp|udp] [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|
host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|eq <SOURCE-PORT>|
host <DEST-HOST-IP>|range <START-PORT> <END-PORT>] [eq [<1-65535>|<SERVICE-NAME>|bgp|dns|
ftp|
ftp-data|gopher|https|ldap|nntp|ntp|pop3|sip|smtp|ssh|telnet|tftp|www]|range <START-PORT>
<END-PORT>]
(log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

|                  |                                                                                                                                                                                           |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| tcp              | Applies this deny rule to TCP packets only                                                                                                                                                |
| udp              | Applies this deny rule to UDP packets only                                                                                                                                                |
| <SOURCE-IP/MASK> | This keyword is common to the ‘tcp’ and ‘udp’ parameters. Specifies the source IP address and mask (A.B.C.D/M) to match. TCP/UDP packets received from the specified sources are dropped. |

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <NETWORK-GROUP-ALIAS-NAME>    | <p>This keyword is common to the 'tcp' and 'udp' parameters. Applies a network-group alias to identify the source IP addresses. TCP/UDP packets received from the sources defined in the network-group alias are dropped.</p> <ul style="list-style-type: none"> <li>• &lt;NETWORK-ALIAS-GROUP-NAME&gt; – Specify the network-group alias name (should be existing and configured).</li> </ul> <p>After specifying the source and destination IP address(es), specify the action taken in case of a match.</p> |
| any                           | <p>This keyword is common to the 'tcp' and 'udp' parameters. Specifies the source as any IP address. TCP/UDP packets received from any source are dropped.</p>                                                                                                                                                                                                                                                                                                                                                 |
| from-vlan <VLAN-ID>           | <p>This keyword is common to the 'tcp' and 'udp' parameters. Specifies a single VLAN or a range of VLANs as the match criteria. TCP/UDP packets received from the VLANs identified here are dropped.</p> <ul style="list-style-type: none"> <li>• &lt;VLAN-ID&gt; – Specify the VLAN ID. To configure a range of VLANs, enter the start and end VLAN IDs separated by a hyphen (for example, 12-20).</li> </ul> <p><b>Note:</b> Use this option with WLANs and port ACLs.</p>                                  |
| host <SOURCE-HOST-IP>         | <p>Identifies a specific host (as the source to match) by its IP address. TCP/UDP packets received from the specified host are dropped.</p> <ul style="list-style-type: none"> <li>• &lt;SOURCE-HOST-IP&gt; – Specify the source host's exact IP address in the A.B.C.D format.</li> </ul>                                                                                                                                                                                                                     |
| <DEST-IP/MASK>                | <p>This keyword is common to the 'tcp' and 'udp' parameters. Sets the destination IP address and mask (A.B.C.D/M) to match. TCP/UDP packets addressed to the specified destinations are dropped.</p>                                                                                                                                                                                                                                                                                                           |
| any                           | <p>This keyword is common to the 'tcp' and 'udp' parameters. Specifies the destination as any destination IP address. TCP/UDP packets received from any destination are dropped.</p>                                                                                                                                                                                                                                                                                                                           |
| eq <SOURCE-PORT>              | <p>Identifies a specific source port</p> <ul style="list-style-type: none"> <li>• &lt;SOURCE-PORT&gt; – Specify the exact source port.</li> </ul>                                                                                                                                                                                                                                                                                                                                                              |
| host <DEST-HOST-IP>           | <p>Identifies a specific host (as the destination to match) by its IP address. TCP/UDP packets addressed to the specified host are dropped.</p> <ul style="list-style-type: none"> <li>• &lt;DEST-HOST-IP&gt; – Specify the destination host's exact IP address in the A.B.C.D format.</li> </ul>                                                                                                                                                                                                              |
| <NETWORK-GROUP-ALIAS-NAME>    | <p>This keyword is common to the 'tcp' and 'udp' parameters. Applies a network-group alias to identify the destination IP addresses. TCP/UDP packets destined to the addresses identified in the network-group alias are dropped.</p> <ul style="list-style-type: none"> <li>• &lt;NETWORK-ALIAS-GROUP-NAME&gt; – Specify the network-group alias name (should be existing and configured).</li> </ul>                                                                                                         |
| range <START-PORT> <END-PORT> | <p>Specifies a range of source ports</p> <ul style="list-style-type: none"> <li>• &lt;START-PORT&gt; – Specify the first port in the range.</li> <li>• &lt;END-PORT&gt; – Specify the last port in the range.</li> </ul>                                                                                                                                                                                                                                                                                       |

|                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>eq [&lt;1-65535&gt;  &lt;SERVICE-NAME&gt;    bgp dns ftp  ftp- data gopher  https  ldap nntp ntp  pop3  sip smtp  ssh telnet  tftp www]</pre> | <p>Identifies a specific destination or protocol port to match</p> <ul style="list-style-type: none"> <li>• &lt;1-65535&gt; – The destination port is designated by its number</li> <li>• &lt;SERVICE-NAME&gt; – Specifies the service name</li> <li>• bgp – The designated BGP (Border Gateway Protocol) protocol port (179)</li> <li>• dns – The designated DNS (Domain Name System) protocol port (53)</li> <li>• ftp – The designated FTP (File Transfer Protocol) protocol port (21)</li> <li>• ftp-data – The designated FTP data port (20)</li> <li>• gopher – The designated GROPER protocol port (70)</li> <li>• https – The designated HTTPS protocol port (443)</li> <li>• ldap – The designated LDAP (Lightweight Directory Access Protocol) protocol port (389)</li> <li>• nntp – The designated NNTP (Network News Transfer Protocol) protocol port (119)</li> <li>• ntp – The designated NTP (Network Time Protocol) protocol port (123)</li> <li>• pop3 – The designated POP3 protocol port (110)</li> <li>• sip – The designated SIP (Session Initiation Protocol) protocol port (5060)</li> <li>• smtp – The designated SMTP (Simple Mail Transfer Protocol) protocol port (25)</li> <li>• ssh – The designated SSH (Secure Shell) protocol port (22)</li> <li>• telnet – The designated Telnet protocol port (23)</li> <li>• tftp – The designated TFTP (Trivial File Transfer Protocol) protocol port (69)</li> <li>• www – The designated www protocol port (80)</li> </ul> |
| <pre>range &lt;START- PORT&gt; &lt;END- PORT&gt;</pre>                                                                                             | <p>Specifies a range of destination ports</p> <ul style="list-style-type: none"> <li>• &lt;START-PORT&gt; – Specify the first port in the range.</li> <li>• &lt;END-PORT&gt; – Specify the last port in the range.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <pre>log</pre>                                                                                                                                     | <p>Logs all deny events matching this entry. If a source and/or destination IP address or port is matched (i.e. a TCP/UDP packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <pre>rule-precedence &lt;1-5000&gt; rule- description &lt;LINE&gt;</pre>                                                                           | <p>The following keywords are recursive and common to all of the above:</p> <ul style="list-style-type: none"> <li>• rule-precedence – Assigns a precedence for this deny rule <ul style="list-style-type: none"> <li>• &lt;1-5000&gt; – Specify a value from 1 - 5000.</li> </ul> </li> </ul> <p><b>Note:</b> Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.</p> <ul style="list-style-type: none"> <li>• rule-description – Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

### Usage Guidelines

Use this command to deny traffic between networks/hosts based on the protocol type selected in the access list configuration. The following protocols are supported:

- IP
- ICMP
- TCP
- UDP
- PROTO (any Internet protocol other than TCP, UDP, and ICMP)

The last ACE (access control entry) in the access list is an implicit deny statement.



---

Whenever the interface receives the packet, its content is checked against the ACEs in the ACL. It is allowed or denied based on the ACL configuration.

- Filtering TCP/UDP allows you to specify port numbers as filtering criteria.
- Select ICMP as the protocol to allow or deny ICMP packets. Selecting ICMP filters ICMP packets based on ICMP type and code.



#### Note

The log option is functional only for router ACL's. The log option displays an informational logging message about the packet that matches the entry sent to the console

---

### Examples

```
nx9500-6C8809(config-ip-acl-test)#deny proto vrrp any any log rule-precedence 600
nx9500-6C8809(config-ip-acl-test)#deny proto ospf any any log rule-precedence 650
nx9500-6C8809(config-ip-acl-test)#show context
ip access-list test
 deny proto vrrp any any log rule-precedence 600
 deny proto ospf any any log rule-precedence 650
nx9500-6C8809(config-ip-acl-test)#
```

#### Using aliases in IP access list.

The following examples show the usage of network-group aliases:

Example 1.

```
rfs4000-229D58(config-ip-acl-bar)#permit ip $foo any rule-precedence 10
```

Example 2.

```
rfs4000-229D58(config-ip-acl-bar)#permit tcp 192.168.100.0/24 $foobar eq ftp rule-
precedence 20
```

Example 3.

```
rfs4000-229D58(config-ip-acl-bar)#deny ip $guest $lab rule-precedence 30
```

- In example 1, network-group alias \$foo is used as a source.
- In example 2, network-group alias \$foobar is used as a destination.
- In example 3, network-group aliases \$guest and \$lab are used as source and destination respectively.

The following examples show the usage of network-service aliases:

Example 4.

```
rfs4000-229D58(config-ip-acl-bar)# permit $kerberos 10.60.20.0/24 $kerberos-servers log
rule-precedence 40
```

Example 5.

```
rfs4000-229D58(config-ip-acl-bar)#permit $Tandem 10.60.20.0/24 $Tandem-servers log rule-
precedence 50
```

In examples 4, and 5:

- The network-service aliases (\$kerberos and \$Tandem) define the destination protocol-port combinations.
- The source network is 10.60.20.0/24.
- The destination network-address combinations are defined by the network-group aliases (\$kerberos-servers and \$Tandem-servers).

## Related Commands

|              |                                                               |
|--------------|---------------------------------------------------------------|
| <b>no</b>    | Removes a specified IP deny access rule                       |
| <b>alias</b> | Creates and configures aliases (network, VLAN, service, etc.) |

### *disable (ipv4-acl)*

Disables an existing deny or permit rule without removing it from the ACL. A disabled rule is inactive and is not used to filter packets.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
disable [deny|insert|permit]
disable [deny|insert [deny|permit]|permit] [<NETWORK-SERVICE-ALIAS-NAME>|dns-name|
icmp|ip|proto|tcp|udp]
disable [deny|insert [deny|permit]|permit] [<NETWORK-SERVICE-ALIAS-NAME>|
dns-name [contains|exact|suffix]|icmp|ip|proto <PROTOCOL-OPTIONS>|tcp|udp]
[<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|host <SOURCE-HOST-
IP>]
[<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|host <DEST-HOST-IP>] (log,mark [8021p <0-7>|
dscp <0-63>],rule-precedence)
```

### Parameters

```
disable [deny|insert [deny|permit]|permit] [<NETWORK-SERVICE-ALIAS-NAME>|
dns-name [contains|exact|suffix]|icmp|ip|proto <PROTOCOL-OPTIONS>|tcp|udp]
[<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|host <SOURCE-HOST-
IP>]
[<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|host <DEST-HOST-IP>] (log,mark [8021p <0-7>|
dscp <0-63>],rule-precedence)
```

|                                            |                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| disable [deny insert [deny permit] permit] | Disables a deny or permit access rule without removing it from the ACL. This command also enables the insertion of a disable deny or permit rule without overwriting an existing rule in the IP ACL.<br><br><b>Note:</b> To disable an existing deny/permit rule, provide the exact values used to configure the deny or permit rule. |
| <NETWORK-SERVICE-ALIAS-NAME>               | Specifies the network-service alias, identified by the <NETWORK-SERVICE-ALIAS-NAME> keyword, associated with the deny/permit rule                                                                                                                                                                                                     |
| dns-name [contains exact suffix]           | Specifies the packets to reject based on the dns-name match. Applies this deny rule to packets based on dns-names specified in the network-service                                                                                                                                                                                    |
| icmp                                       | Disables a rule applicable to ICMP packets only                                                                                                                                                                                                                                                                                       |
| ip                                         | Disables a rule applicable to IP packets only                                                                                                                                                                                                                                                                                         |
| proto <PROTOCOL-OPTIONS>                   | Disables a rule applicable to any Internet protocol other than TCP, UDP, or ICMP packets. <ul style="list-style-type: none"><li>• &lt;PROTOCOL-OPTIONS&gt; - Identify the Internet protocol using the options available.</li></ul>                                                                                                    |

|                                 |                                                                                                                                                                                                                                                                                                 |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| tcp                             | Disables a rule applicable to TCP packets only                                                                                                                                                                                                                                                  |
| udp                             | Disables a rule applicable to UDP packets only<br><br><b>Note:</b> After specifying the packet type, specify the source and destination devices and network address(es) to match.                                                                                                               |
| <SOURCE-IP/MASK>                | Specify the source IP address and mask in the A.B.C.D/M format.                                                                                                                                                                                                                                 |
| <NETWORK-GROUP-ALIAS-NAME>      | Specifies the network-group alias, identified by the <NETWORK-GROUP-ALIAS-NAME> keyword, associated with this deny/permit rule                                                                                                                                                                  |
| any                             | Select 'any' if the rule is applicable to any source IP address.                                                                                                                                                                                                                                |
| from-vlan <VLAN-ID>             | Specify the VLAN IDs.                                                                                                                                                                                                                                                                           |
| host <SOURCE-HOST-IP>           | Specify the source host's exact IP address.                                                                                                                                                                                                                                                     |
| <DEST-IP/MASK>                  | Specify the destination IP address and mask in the A.B.C.D/M format.                                                                                                                                                                                                                            |
| <NETWORK-GROUP-ALIAS-NAME>      | Specifies the network-group alias, identified by the <NETWORK-GROUP-ALIAS-NAME> keyword, associated with this deny/permit rule                                                                                                                                                                  |
| any                             | Select 'any' if the rule is applicable to any destination IP address.                                                                                                                                                                                                                           |
| host <DEST-HOST-IP>             | Specify the destination host's exact IP address.                                                                                                                                                                                                                                                |
| log                             | Select log, if the rule has been configured to log records in case of a match.                                                                                                                                                                                                                  |
| mark [8021p <0-7>  dscp <0-63>] | Specifies packets to mark <ul style="list-style-type: none"> <li>8021p &lt;0-7&gt; - Marks packets by modifying 802.1p VLAN user priority</li> <li>dscp &lt;0-63&gt; - Marks packets by modifying DSCP TOS bits in the header</li> </ul>                                                        |
| rule-precedence <1-5000>        | Specify the rule precedence. The deny or permit rule with the specified precedence is disabled.<br><br><b>Note:</b> To enable a disabled rule, enter the rule again without the 'disable' keyword.<br><br><b>Note:</b> The <b>no &gt; disable</b> command removes a disabled rule from the ACL. |

## Examples

The following example shows the 'auto-tunnel-acl' settings before the disable command is executed:

```

nx9500-6C8809(config-ip-acl-auto-tunnel-acl)#show context
ip access-list auto-tunnel-acl
 deny ip host 200.200.200.99 30.30.30.1/24 rule-precedence 2
 permit ip host 200.200.200.99 any rule-precedence 3
nx9500-6C8809(config-ip-acl-auto-tunnel-acl)#
nx9500-6C8809(config-ip-acl-auto-tunnel-acl)#disable permit ip host 200.200.200.99 any
rule-precedence 3

```

The following example shows the 'auto-tunnel-acl' settings after the disable command is executed:

```

nx9500-6C8809(config-ip-acl-auto-tunnel-acl)#show context
ip access-list auto-tunnel-acl
 deny ip host 200.200.200.99 30.30.30.1/24 rule-precedence 2
 disable permit ip host 200.200.200.99 any rule-precedence 3
nx9500-6C8809(config-ip-acl-auto-tunnel-acl)#
rfs4000-229D58(config-ip-acl-test)#deny icmp any any log rule-precedence 1
rfs4000-229D58(config-ip-acl-test)#show context
ip access-list test

```

```

deny icmp any any rule-precedence 1
rfs4000-229D58(config-ip-acl-test)#
rfs4000-229D58(config-ip-acl-test)#disable deny icmp any any rule-precedence 1
rfs4000-229D58(config-ip-acl-test)#show context
ip access-list test
deny tcp from-vlan 1 any any rule-precedence 1
permit icmp any host 192.168.13.7 1 1 rule-precedence 2
rfs4000-229D58(config-ip-acl-test)#
rfs4000-229D58(config-ip-acl-test)#disable insert deny ip any any log rule-precedence 2
rfs4000-229D58(config-ip-acl-test)#show context
ip access-list test
deny tcp from-vlan 1 any any rule-precedence 1
deny ip any any log rule-precedence 2
permit icmp any host 192.168.13.7 1 1 rule-precedence 3
rfs4000-229D58(config-ip-acl-test)#

```

In the following example a disable deny rule has been inserted in the IP ACL “test”:

```

rfs4000-229D58(config-ip-acl-test)#show context
ip access-list test
deny tcp from-vlan 1 any any rule-precedence 1
permit icmp any host 192.168.13.7 1 1 rule-precedence 2
rfs4000-229D58(config-ip-acl-test)#
rfs4000-229D58(config-ip-acl-test)#disable insert deny ip any any log rule-precedence 2
rfs4000-229D58(config-ip-acl-test)#show context
ip access-list test
deny tcp from-vlan 1 any any rule-precedence 1
deny ip any any log rule-precedence 2
permit icmp any host 192.168.13.7 1 1 rule-precedence 3
rfs4000-229D58(config-ip-acl-test)#

```

### Related Commands

|               |                                                                 |
|---------------|-----------------------------------------------------------------|
| <b>no</b>     | Enables a disabled deny or permit rule                          |
| <b>deny</b>   | Creates a new deny access rule or modifies an existing rule     |
| <b>permit</b> | Creates a new permit access rule or modifies an existing rule   |
| <b>alias</b>  | Creates and configures a aliases (network, VLAN, service, etc.) |

### *insert (ipv4-acl)*

Enables the insertion of a rule in an IP ACL without overwriting or replacing an existing rule having the same precedence

The insert option allows a new rule to be inserted within a IP access list. Consider an IP ACL consisting of rules having precedences 1, 2, 3, 4, 5, and 6. You want to insert a new rule with precedence 4, without overwriting the existing precedence 4 rule. Using the insert option inserts the new rule prior to the existing one. The existing precedence 4 rule’s precedence changes to 5, and the change cascades down the list of rules within the ACL. That means rule 5 becomes rule 6, and rule 6 becomes rule 7.



#### Note

NOT using *insert* when creating a new rule having the same precedence as an existing rule overwrites the existing rule.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
insert [deny|permit] <PARAMETERS> (log,mark [8021p <0-7>|dscp <0-63>],rule-precedence <1-5000>)
{(rule-description <LINE>)}
```

## Parameters

```
insert [deny|permit] <PARAMETERS> (log,mark [8021p <0-7>|dscp <0-63>],rule-precedence <1-5000>)
{(rule-description <LINE>)}
```

|                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [deny permit]                                        | Inserts a deny or a permit rule within an IP ACL                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <PARAMETERS>                                         | Provide the match criteria for this deny/permit rule. Packets will be filtered based on the criteria set here.<br>For more information on the deny rule, see <a href="#">deny</a> .<br>For more information on the permit rule, see <a href="#">permit</a> .                                                                                                                                                                                                                                       |
| log                                                  | After specifying the match criteria, specify the action taken for filtered packets<br>Logs all deny/permit events matching this entry. If a source and/or destination IP address is matched an event is logged.                                                                                                                                                                                                                                                                                    |
| mark [8021p <0-7> <br>dscp <0-63>]                   | Specifies packets to mark <ul style="list-style-type: none"><li>8021p &lt;0-7&gt; - Marks packets by modifying 802.1p VLAN user priority</li><li>dscp &lt;0-63&gt; - Marks packets by modifying DSCP TOS bits in the header</li></ul>                                                                                                                                                                                                                                                              |
| rule-precedence <1-5000> rule-<br>description <LINE> | Assigns a precedence for this deny/permit rule <ul style="list-style-type: none"><li>&lt;1-5000&gt; - Specify a value from 1 - 5000.<br/><b>Note:</b> Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.</li><li>rule-description - Optional. Configures a description for this deny/permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).</li></ul> |



### Note

The log option is functional only for router ACL's. The log option displays an informational logging message about the packet that matches the entry sent to the console.

## Examples

```
rfs4000-229D58(config-ip-acl-test)#deny tcp from-vlan 1 any any rule-precedence 1
rfs4000-229D58(config-ip-acl-test)#permit icmp any host 192.168.13.7 1 1 rule-precedence 2
rfs4000-229D58(config-ip-acl-test)#show context
ip access-list test
 deny tcp from-vlan 1 any any rule-precedence 1
 permit icmp any host 192.168.13.7 1 1 rule-precedence 2
rfs4000-229D58(config-ip-acl-test)#
```

In the following example a new rule is inserted between the rules having precedences 1 and 2. The precedence of the existing precedence '2' rule changes to precedence 3.

```
rfs4000-229D58(config-ip-acl-test)#insert deny ip any any rule-precedence 2
rfs4000-229D58(config-ip-acl-test)#show context
ip access-list test
 deny tcp from-vlan 1 any any rule-precedence 1
 deny ip any any rule-precedence 2
 permit icmp any host 192.168.13.7 1 1 rule-precedence 3
rfs4000-229D58(config-ip-acl-test)#
```

## Related Commands

|              |                                                               |
|--------------|---------------------------------------------------------------|
| <b>alias</b> | Creates and configures aliases (network, VLAN, service, etc.) |
|--------------|---------------------------------------------------------------|

### *permit (ipv4-acl)*

Creates a permit rule that marks packets (from a specified source IP and/or to a specified destination IP) for forwarding. You can also use this command to modify an existing permit rule.



#### Note

Use a decimal value representation to implement a permit/deny designation for a packet. The command set for IP ACLs provides the hexadecimal values for each listed EtherType. Use the decimal equivalent of the EtherType listed for any other EtherType.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
permit [<NETWORK-SERVICE-ALIAS-NAME>|dns-name|icmp|ip|proto|tcp|udp]
permit <NETWORK-SERVICE-ALIAS-NAME> [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|
any|from-vlan <VLAN-ID>|host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|any|host <DEST-HOST-IP>|
<NETWORK-GROUP-ALIAS-NAME>] (log,mark [8021p <0-7>|dscp <0-63>],rule-precedence <1-5000>)
{(rule-description <LINE>)}
permit dns-name [contains|exact|suffix]permit dns-name [contains|exact|suffix]
permit dns-name [contains|exact|suffix] <WORD> (log,rule-precedence <1-5000>)
{(rule-description <LINE>)}
permit dns-name exact <WORD> (log,mark [8021p <0-7>|dscp <0-63>],rule-precedence <1-5000>)
{(rule-description <LINE>)}
permit icmp [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|
host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|host <DEST-HOST-IP>]
(<ICMP-TYPE> <ICMP-CODE>,log,rule-precedence <1-5000>) {(rule-description <LINE>)}
permit ip [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|
host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|host <DEST-HOST-IP>]
(log,rule-precedence <1-5000>) {(rule-description <LINE>)}
permit proto [<PROTOCOL-NUMBER>|<PROTOCOL-NAME>|eigrp|gre|igmp|igp|ospf|vrrp]
[<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|host <SOURCE-HOST-
IP>]
[<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|host <DEST-HOST-IP>] (log,rule-precedence
<1-5000>)
{(rule-description <LINE>)}
permit [tcp|udp] [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|
host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|eq <SOURCE-PORT>|
host <DEST-HOST-IP>|
range <START-PORT> <END-PORT>] [eq [<1-65535>|<SERVICE-NAME>|bgp|dns|ftp|ftp-data|gopher|
https|ldap|nntp|ntp|pop3|
sip|smtp|ssh|telnet|tftp|www]|range <START-PORT> <END-PORT>] (log,rule-precedence
<1-5000>)
{(rule-description <LINE>)}

```

### Parameters

```
permit <NETWORK-SERVICE-ALIAS-NAME> [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|
any|from-vlan <VLAN-ID>|host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|any|host <DEST-HOST-IP>|
```

```
<NETWORK-GROUP-ALIAS-NAME>] (log,mark [8021p <0-7>|dscp <0-63>],rule-precedence <1-5000>)
{(rule-description <LINE>)}
```

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <NETWORK-SERVICE-ALIAS-NAME> | <p>Applies this permit rule to packets based on service protocols and ports specified in the network-service alias</p> <ul style="list-style-type: none"> <li>• &lt;NETWORK-SERVICE-ALIAS-NAME&gt; – Specify the network-service alias name (should be existing and configured).</li> </ul> <p>A network-service alias defines service protocols and ports to match. When used with an ACL, the network-service alias defines the service-specific components of the ACL permit rule.</p> <p><b>Note:</b> For more information on configuring network-service alias, see <a href="#">alias</a>.</p>                                               |
| <SOURCE-IP/MASK>             | <p>Specifies the source IP address and mask (A.B.C.D/M) to match. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified network are permitted.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <NETWORK-GROUP-ALIAS-NAME>   | <p>Applies a network-group alias to identify the source IP addresses. Packets, matching the service protocols and ports specified in the network-service alias, received from the addresses identified by the network-group alias are permitted.</p> <ul style="list-style-type: none"> <li>• &lt;NETWORK-GROUP-ALIAS-NAME&gt; – Specify the network-group alias name (should be existing and configured).</li> </ul> <p>A network-group alias defines a single or a range of addresses of devices, hosts, and networks. When used with an ACL, the network-group alias defines the network-specific component of the ACL rule (permit/deny).</p> |
| any                          | <p>Specifies the source as any source IP address. Packets, matching the service protocols and ports specified in the network-service alias, received from any source are permitted.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| from-vlan <VLAN-ID>          | <p>Specifies a single VLAN or a range of VLANs as the match criteria. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified VLAN(s) are permitted.</p> <ul style="list-style-type: none"> <li>• &lt;VLAN-ID&gt; – Specify the VLAN ID. To configure a range of VLANs, enter the start and end VLAN IDs separated by a hyphen (for example, 12-20).</li> </ul> <p><b>Note:</b> Use this option with WLANs and port ACLs.</p>                                                                                                                                                       |
| host <SOURCE-HOST-IP>        | <p>Identifies a specific host (as the source to match) by its IP address. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified host are permitted.</p> <ul style="list-style-type: none"> <li>• &lt;SOURCE-HOST-IP&gt; – Specify the source host's exact IP address in the A.B.C.D format.</li> </ul>                                                                                                                                                                                                                                                                            |
| <DEST-IP/MASK>               | <p>Specifies the destination IP address and mask (A.B.C.D/M) to match. Packets, matching the service protocols and ports specified in the network-service alias, addressed to the specified network are permitted.</p>                                                                                                                                                                                                                                                                                                                                                                                                                            |
| any                          | <p>Specifies the destination as any destination IP address. Packets, matching the service protocols and ports specified in the network-service alias, addressed to any destination are permitted.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| host <DEST-HOST-IP>          | <p>Identifies a specific host (as the destination to match) by its IP address. Packets, matching the service protocols and ports specified in the network-service alias, addressed to the specified host are permitted.</p> <ul style="list-style-type: none"> <li>• &lt;DEST-HOST-IP&gt; – Specify the destination host's exact IP address in the A.B.C.D format.</li> </ul>                                                                                                                                                                                                                                                                     |

|                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <NETWORK-GROUP-ALIAS-NAME>                       | <p>Applies a network-group alias to identify the destination IP addresses. Packets, matching the service protocols and ports specified in the network-service alias, destined for the addresses identified by the network-group alias are permitted.</p> <ul style="list-style-type: none"> <li>• &lt;NETWORK-GROUP-ALIAS-NAME&gt; – Specify the network-group alias name (should be existing and configured).</li> </ul>                                                                                                                                                                                                                                        |
| log                                              | <p>Logs all permit events matching this entry. If a source and/or destination IP address is matched (i.e. if any specified type of packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged.</p>                                                                                                                                                                                                                                                                                                                                                                                                        |
| mark [8021p <0-7>] dscp <0-63>]                  | <p>Specifies packets to mark</p> <ul style="list-style-type: none"> <li>• 8021p &lt;0-7&gt; – Marks packets by modifying 802.1p VLAN user priority</li> <li>• dscp &lt;0-63&gt; – Marks packets by modifying DSCP TOS bits in the header</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                              |
| rule-precedence <1-5000> rule-description <LINE> | <p>The following keywords are recursive and common to all of the above parameters:</p> <ul style="list-style-type: none"> <li>• rule-precedence – Assigns a precedence for this permit rule <ul style="list-style-type: none"> <li>• &lt;1-5000&gt; – Specify a value from 1 - 5000.</li> </ul> <p><b>Note:</b> Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.</p> </li> <li>• rule-description – Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).</li> </ul> |

```
permit dns-name [contains|exact (mark)|suffix] <WORD> (log,rule-precedence <1-5000>)
{(rule-description <LINE>)}
```

|                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dns-name                                            | Applies this permit rule to packets based on dns-names specified in the network-service                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| contains                                            | Matches any hostname which has this DNS label. (for example, *.test.*)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| exact                                               | Matches an exact hostname as specified in the network-service                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| suffix                                              | Matches any hostname as suffix (for example, *.test)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <WORD>                                              | Identifies a specific host (as the source to match) by its domain name. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified host are forwarded.                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| log                                                 | Logs all permit events matching this dns entry. If a dns-name is matched an event is logged.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| rule-precedence <1-5000><br>rule-description <LINE> | <p>The following keywords are recursive and common to all of the above parameters:</p> <ul style="list-style-type: none"> <li>• rule-precedence – Assigns a precedence for this permit rule <ul style="list-style-type: none"> <li>• &lt;1-5000&gt; – Specify a value from 1 - 5000.</li> </ul> <p><b>Note:</b> Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.</p> </li> <li>• rule-description – Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).</li> </ul> |

```
permit icmp [<SOURCE-IP/MASK>|<NETWORK-GROUP-NAME>|any|from-vlan <VLAN-ID>|
host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-NAME>|any|host <DEST-HOST-IP>]
(<ICMP-TYPE> <ICMP-CODE> ,log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```



|                            |                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| icmp                       | Applies this permit rule to ICMP packets only                                                                                                                                                                                                                                                                                                                                                               |
| <SOURCE-IP/MASK>           | Specifies the source IP address and mask (A.B.C.D/M) to match. ICMP packets received from the specified sources are permitted.                                                                                                                                                                                                                                                                              |
| <NETWORK-GROUP-ALIAS-NAME> | Applies a network-group alias to identify the source IP addresses. ICMP packets received from the addresses identified by the network-group alias are permitted. <ul style="list-style-type: none"> <li>• &lt;NETWORK-GROUP-ALIAS-NAME&gt; – Specify the network-group alias name (should be existing and configured).</li> </ul>                                                                           |
| any                        | Specifies the source as any IP address. ICMP packets received from any source are permitted.                                                                                                                                                                                                                                                                                                                |
| from-vlan <VLAN-ID>        | Specifies a single VLAN or a range of VLANs as the match criteria. ICMP packets received from the VLANs identified here are permitted. <ul style="list-style-type: none"> <li>• &lt;VLAN-ID&gt; – Specify the VLAN ID. To configure a range of VLANs, enter the start and end VLAN IDs separated by a hyphen (for example, 12-20).</li> </ul> <p><b>Note:</b> Use this option with WLANs and port ACLs.</p> |
| host <SOURCE-HOST-IP>      | Identifies a specific host (as the source to match) by its IP address. ICMP packets received from the specified host are permitted. <ul style="list-style-type: none"> <li>• &lt;SOURCE-HOST-IP&gt; – Specify the source host's exact IP address in the A.B.C.D format.</li> </ul>                                                                                                                          |
| <DEST-IP/MASK>             | Specifies the destination IP address and mask (A.B.C.D/M) to match. ICMP packets addressed to specified destinations are permitted.                                                                                                                                                                                                                                                                         |
| <NETWORK-GROUP-ALIAS-NAME> | Applies a network-group alias to identify the destination IP addresses. ICMP packets destined for addresses identified by the network-group alias are permitted. <ul style="list-style-type: none"> <li>• &lt;NETWORK-GROUP-ALIAS-NAME&gt; – Specify the network-group alias name (should be existing and configured).</li> </ul>                                                                           |
| any                        | Specifies the destination as any IP address. ICMP packets addressed to any destination are permitted.                                                                                                                                                                                                                                                                                                       |
| host <DEST-HOST-IP>        | Identifies a specific host (as the destination to match) by its IP address. ICMP packets addressed to the specified host are permitted. <ul style="list-style-type: none"> <li>• &lt;DEST-HOST-IP&gt; – Specify the destination host's exact IP address in the A.B.C.D format.</li> </ul>                                                                                                                   |
| <ICMP-TYPE>                | Defines the ICMP packet type<br>For example, an ICMP type 0 indicates it is an ECHO REPLY, and type 8 indicates it is an ECHO.                                                                                                                                                                                                                                                                              |
| <ICMP-CODE>                | Defines the ICMP message type<br>For example, an ICMP code 3 indicates "Destination Unreachable", code 1 indicates "Host Unreachable", and code 3 indicates "Port Unreachable."<br><br><b>Note:</b> After specifying the source and destination IP address(es), the ICMP message type, and the ICMP code, specify the action taken in case of a match.                                                      |

|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| log                                                     | Logs all permit events matching this entry. If a source and/or destination IP address is matched (i.e. a ICMP packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged.                                                                                                                                                                                                                                                                                                                                                                                                                          |
| rule-precedence<br><1-5000> rule-<br>description <LINE> | <p>The following keywords are recursive and common to all of the above parameters:</p> <ul style="list-style-type: none"> <li>rule-precedence – Assigns a precedence for this permit rule</li> <li>&lt;1-5000&gt; – Specify a value from 1 - 5000.</li> </ul> <p><b>Note:</b> Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.</p> <ul style="list-style-type: none"> <li>rule-description – Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).</li> </ul> |

```
permit ip [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|
host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|host <DEST-HOST-IP>]
(log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

|                                    |                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip                                 | Applies this permit rule to IP packets only                                                                                                                                                                                                                                                                                                                                                                 |
| <SOURCE-IP/<br>MASK>               | Specifies the source IP address and mask (A.B.C.D/M) to match. IP packets received from the specified networks are permitted.                                                                                                                                                                                                                                                                               |
| <NETWORK-<br>GROUP-ALIAS-<br>NAME> | <p>Applies a network-group alias to identify the source IP addresses. IP packets received from the addresses identified by the network-group alias are permitted.</p> <ul style="list-style-type: none"> <li>&lt;NETWORK-GROUP-ALIAS-NAME&gt; – Specify the network-group alias name (should be existing and configured).</li> </ul>                                                                        |
| any                                | Specifies the source as any source IP address. IP packets received from any source are permitted.                                                                                                                                                                                                                                                                                                           |
| from-vlan <VLAN-<br>ID>            | <p>Specifies a single VLAN or a range of VLANs as the match criteria. IP packets received from the specified VLANs are permitted.</p> <ul style="list-style-type: none"> <li>&lt;VLAN-ID&gt; – Specify the VLAN ID. To configure a range of VLAN IDs, enter the start and end VLAN IDs separated by a hyphen (for example, 12-20).</li> </ul> <p><b>Note:</b> Use this option with WLANs and port ACLs.</p> |
| host <SOURCE-<br>HOST-IP>          | <p>Identifies a specific host (as the source to match) by its IP address. IP packets received from the specified host are permitted.</p> <ul style="list-style-type: none"> <li>&lt;SOURCE-HOST-IP&gt; – Specify the source host's exact IP address in the A.B.C.D format.</li> </ul>                                                                                                                       |
| <DEST-IP/MASK>                     | Specifies the destination IP address and mask (A.B.C.D/M) to match. IP packets addressed to the specified networks are permitted.                                                                                                                                                                                                                                                                           |
| any                                | Specifies the destination as any destination IP address. IP packets addressed to any destination are permitted.                                                                                                                                                                                                                                                                                             |
| host <DEST-HOST-<br>IP>            | <p>Identifies a specific host (as the destination to match) by its IP address. IP packets addressed to the specified host are permitted.</p> <ul style="list-style-type: none"> <li>&lt;DEST-HOST-IP&gt; – Specify the destination host's exact IP address in the A.B.C.D format.</li> </ul>                                                                                                                |
| <NETWORK-<br>GROUP-ALIAS-<br>NAME> | <p>Applies a network-group alias to identify the source IP addresses. IP packets destined for addresses identified by the network-group alias are permitted.</p> <ul style="list-style-type: none"> <li>&lt;NETWORK-GROUP-ALIAS-NAME&gt; – Specify the network-group alias name (should be existing and configured).</li> </ul>                                                                             |

|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| log                                                     | Logs all permit events matching this entry. If a source and/or destination IP address is matched (i.e. a IP packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged.                                                                                                                                                                                                                                                                                                                                                                                                                            |
| rule-precedence<br><1-5000> rule-<br>description <LINE> | <p>The following keywords are recursive and common to all of the above parameters:</p> <ul style="list-style-type: none"> <li>rule-precedence – Assigns a precedence for this permit rule</li> <li>&lt;1-5000&gt; – Specify a value from 1 - 5000.</li> </ul> <p><b>Note:</b> Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.</p> <ul style="list-style-type: none"> <li>rule-description – Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).</li> </ul> |

```

permit proto [<PROTOCOL-NUMBER>|<PROTOCOL-NAME>|eigrp|gre|igmp|igp|ospf|vrrp]
[<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|host <SOURCE-HOST-IP>]
[<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|host <DEST-HOST-IP>] (log,rule-precedence
<1-5000>)
{(rule-description <LINE>)}

```

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| proto             | Configures the ACL for additional protocols<br>Additional protocols (other than IP, ICMP, TCP, and UDP) must be configured using this parameter                                                                                                                                                                                                                                                                                                                                                    |
| <PROTOCOL-NUMBER> | Filters protocols using their IANA protocol number <ul style="list-style-type: none"> <li>&lt;PROTOCOL-NUMBER&gt; – Specify the protocol number.</li> </ul>                                                                                                                                                                                                                                                                                                                                        |
| <PROTOCOL-NAME>   | Filters protocols using their IANA protocol name <ul style="list-style-type: none"> <li>&lt;PROTOCOL-NAME&gt; – Specify the protocol name.</li> </ul>                                                                                                                                                                                                                                                                                                                                              |
| eigrp             | Identifies the EIGRP protocol (number 88)<br>EIGRP enables routers to maintain copies of neighbors' routing tables. Routers use this information to determine the fastest route to a destination. When a router fails to find a route in its stored route tables, it sends a query to neighbors who in turn query their neighbors till a route is found. EIGRP also enables routers to inform neighbors of changes in their routing tables.                                                        |
| gre               | Identifies the GRE protocol (number 47)<br>GRE is a tunneling protocol that enables transportation of protocols (IP, IPX, DEC net, etc.) over an IP network. GRE encapsulates the packet at the source and removes the encapsulation at the destination.                                                                                                                                                                                                                                           |
| igmp              | Identifies the IGMP protocol (number 2)<br>IGMP establishes and maintains multicast group memberships to interested members. Multicasting allows a networked computer to send content to multiple computers who have registered to receive the content. IGMP snooping is for listening to IGMP traffic between an IGMP host and routers in the network to maintain a map of the links that require multicast streams. Multicast traffic is filtered out for those links which do not require them. |
| igp               | Identifies any private internal gateway (primarily used by CISCO for their IGRP) (number 9)<br>IGP enables exchange of information between hosts and routers within a managed network. The most commonly used IGP protocols are: RIP and OSPF                                                                                                                                                                                                                                                      |

|                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ospf                               | Identifies the OSPF protocol (number 89)<br>OSPF is a link-state IGP. OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets.                                                      |
| vrrp                               | Identifies the VRRP protocol (number 112)<br>VRRP allows a pool of routers to be advertised as a single virtual router. This virtual router is configured by hosts as their default gateway. VRRP elects a master router, from this pool, and assigns it a virtual IP address. The master router routes and forwards packets to hosts on the same subnet. When the master router fails, one of the backup routers is elected as the master and its IP address is mapped to the virtual IP address. |
| <SOURCE-IP/<br>MASK>               | Specifies the source IP address and mask (A.B.C.D/M) to match. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the specified sources are permitted.                                                                                                                                                                                                                                                                                                                                   |
| <NETWORK-<br>GROUP-ALIAS-<br>NAME> | Applies a network-group alias to identify the source IP addresses. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the sources defined in the network-group alias are permitted. <ul style="list-style-type: none"> <li>• &lt;NETWORK-GROUP-ALIAS-NAME&gt; - Specify the network-group alias name (should be existing and configured).</li> </ul>                                                                                                                                     |
| any                                | Specifies the source as any IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from any source are permitted.                                                                                                                                                                                                                                                                                                                                                                     |
| from-vlan<br><VLAN-ID>             | Specifies a single VLAN or a range of VLANs as the match criteria. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the VLANs identified here are permitted. <ul style="list-style-type: none"> <li>• &lt;VLAN-ID&gt; - Specify the VLAN ID. A range of VLANs is represented by the start and end VLAN IDs separated by a hyphen (for example, 12-20).</li> </ul> <p><b>Note:</b> Use this option with WLANs and port ACLs.</p>                                                        |
| host <SOURCE-<br>HOST-IP>          | Identifies a specific host (as the source to match) by its IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the specified host are permitted. <ul style="list-style-type: none"> <li>• &lt;SOURCE-HOST-IP&gt; - Specify the source host's exact IP address in the A.B.C.D format.</li> </ul>                                                                                                                                                                               |
| <DEST-IP/MASK>                     | Specifies the destination IP address and mask (A.B.C.D/M) to match. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to the specified destinations are permitted.                                                                                                                                                                                                                                                                                                                          |
| any                                | Specifies the destination as any destination IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to any destination are permitted.                                                                                                                                                                                                                                                                                                                                                |
| host <DEST-<br>HOST-IP>            | Identifies a specific host (as the destination to match) by its IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addresses to the specified host are permitted. <ul style="list-style-type: none"> <li>• &lt;SOURCE-HOST-IP&gt; - Specify the destination host's exact IP address in the A.B.C.D format.</li> </ul>                                                                                                                                                                      |
| <NETWORK-<br>GROUP-ALIAS-<br>NAME> | Applies a network-group alias to identify the destination IP addresses. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to the destinations identified in the network-group alias are permitted. <ul style="list-style-type: none"> <li>• &lt;NETWORK-ALIAS-NAME&gt; - Specify the network-group alias name (should be existing and configured).</li> </ul> <p>After specifying the source and destination IP address(es), specify the action taken in case of a match.</p>               |

|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| log                                                        | Logs all permit events matching this entry. If a source and/or destination IP address is matched (i.e. a packet (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) is received from a specified IP address and/or is destined for a specified IP address), an event is logged.                                                                                                                                                                                                                                                                                                                                                                                         |
| rule-precedence<br><1-5000> rule-<br>description<br><LINE> | <p>The following keywords are recursive and common to all of the above parameters:</p> <ul style="list-style-type: none"> <li>rule-precedence – Assigns a precedence for this permit rule <ul style="list-style-type: none"> <li>&lt;1-5000&gt; – Specify a value from 1 - 5000.</li> </ul> <p><b>Note:</b> Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.</p> </li> <li>rule-description – Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).</li> </ul> |

```

permit [tcp|udp] [<SOURCE-IP/MASK> | <NETWORK-GROUP-ALIAS-NAME> | any | from-vlan <VLAN-ID> |
host <SOURCE-HOST-IP>] [<DEST-IP/MASK> | <NETWORK-GROUP-ALIAS-NAME> | any | eq <SOURCE-PORT> |
host <DEST-HOST-IP> | range <START-PORT> <END-PORT>] [eq [<1-65535> | <SERVICE-NAME> | bgp | dns |
ftp |
ftp-data | gopher | https | ldap | nntp | ntp | pop3 | sip | smtp | ssh | telnet | tftp | www] | range <START-PORT>
<END-PORT>] (log, rule-precedence <1-5000>) { (rule-description <LINE>) }

```

|                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| tcp                                | Applies this permit rule to TCP packets only                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| udp                                | Applies this permit rule to UDP packets only                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <SOURCE-IP/<br>MASK>               | This keyword is common to the 'tcp' and 'udp' parameters. Specifies the source IP address and mask (A.B.C.D/M) to match. TCP/UDP packets received from the specified sources are permitted.                                                                                                                                                                                                                                                                                               |
| <NETWORK-<br>GROUP-ALIAS-<br>NAME> | <p>This keyword is common to the 'tcp' and 'udp' parameters. Applies a network-group alias to identify the source IP addresses. TCP/UDP packets received from the VLANs identified here are permitted.</p> <ul style="list-style-type: none"> <li>&lt;NETWORK-ALIAS-GROUP-NAME&gt; – Specify the network-group alias name (should be existing and configured).</li> </ul> <p>After specifying the source and destination IP address(es), specify the action taken in case of a match.</p> |
| any                                | This keyword is common to the 'tcp' and 'udp' parameters. Specifies the source as any source IP address. TCP/UDP packets received from any source are permitted.                                                                                                                                                                                                                                                                                                                          |
| from-vlan <VLAN-<br>ID>            | <p>This keyword is common to the 'tcp' and 'udp' parameters. Specifies a single VLAN or a range of VLANs as the match criteria. TCP/UDP packets received from the VLANs identified here are permitted.</p> <ul style="list-style-type: none"> <li>&lt;VLAN-ID&gt; – Specify the VLAN ID. To configure a range of VLANs, enter the start and end VLAN IDs separated by a hyphen (for example, 12-20).</li> </ul> <p><b>Note:</b> Use this option with WLANs and port ACLs.</p>             |
| host <SOURCE-<br>HOST-IP>          | <p>Identifies a specific host (as the source to match) by its IP address. TCP/UDP packets received from the specified host are permitted.</p> <ul style="list-style-type: none"> <li>&lt;SOURCE-HOST-IP&gt; – Specify the source host's exact IP address in the A.B.C.D format.</li> </ul>                                                                                                                                                                                                |
| <DEST-IP/MASK>                     | This keyword is common to the 'tcp' and 'udp' parameters. Sets the destination IP address and mask (A.B.C.D/M) to match. TCP/UDP packets addressed to the specified destinations are permitted.                                                                                                                                                                                                                                                                                           |

|                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| any                                                                                                             | This keyword is common to the 'tcp' and 'udp' parameters. Specifies the destination as any destination IP address. TCP/UDP packets received from any destination are permitted.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| eq <SOURCE-PORT>                                                                                                | Identifies a specific source port <ul style="list-style-type: none"> <li>• &lt;SOURCE-PORT&gt; – Specify the exact source port.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| host <DEST-HOST-IP>                                                                                             | Identifies a specific host (as the destination to match) by its IP address. TCP/UDP packets addressed to the specified host are permitted. <ul style="list-style-type: none"> <li>• &lt;DEST-HOST-IP&gt; – Specify the destination host's exact IP address in the A.B.C.D format.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <NETWORK-GROUP-ALIAS-NAME>                                                                                      | This keyword is common to the 'tcp' and 'udp' parameters. Applies a network-group alias to identify the destination IP addresses. TCP/UDP packets destined to the addresses identified in the network-group alias are permitted. <ul style="list-style-type: none"> <li>• &lt;NETWORK-ALIAS-GROUP-NAME&gt; – Specify the network-group alias name (should be existing and configured).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| eq [<1-65535> <SERVICE-NAME> bgp dns ftp ftp-data gopher https ldap nntp ntp pop3 sip smtp ssh telnet tftp www] | Identifies a specific destination or protocol port to match <ul style="list-style-type: none"> <li>• &lt;1-65535&gt; – The destination port is designated by its number</li> <li>• &lt;SERVICE-NAME&gt; – Specifies the service name</li> <li>• bgp – The designated BGP protocol port (179)</li> <li>• dns – The designated DNS protocol port (53)</li> <li>• ftp – The designated FTP protocol port (21)</li> <li>• ftp-data – The designated FTP data port (20)</li> <li>• gopher – The designated GROPHER protocol port (70)</li> <li>• https – The designated HTTPS protocol port (443)</li> <li>• ldap – The designated LDAP protocol port (389)</li> <li>• nntp – The designated NNTP protocol port (119)</li> <li>• ntp – The designated NTP protocol port (123)</li> <li>• pop3 – The designated POP3 protocol port (110)</li> <li>• sip – The designated SIP protocol port (5060)</li> <li>• smtp – The designated SMTP protocol port (25)</li> <li>• ssh – The designated SSH protocol port (22)</li> <li>• telnet – The designated Telnet protocol port (23)</li> <li>• tftp – The designated TFTP protocol port (69)</li> <li>• www – The designated www protocol port (80)</li> </ul> |
| range <START-PORT> <END-PORT>                                                                                   | Specifies a range of destination ports <ul style="list-style-type: none"> <li>• &lt;START-PORT&gt; – Specify the first port in the range.</li> <li>• &lt;END-PORT&gt; – Specify the last port in the range.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| log                                                     | Logs all permit events matching this entry. If a source and/or destination IP address or port is matched (i.e. a TCP/UDP packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged.                                                                                                                                                                                                                                                                                                                                                                                                    |
| rule-precedence<br><1-5000> rule-<br>description <LINE> | <p>The following keywords are recursive and common to all of the above:</p> <ul style="list-style-type: none"> <li>rule-precedence – Assigns a precedence for this permit rule</li> <li>&lt;1-5000&gt; – Specify a value from 1 - 5000.</li> </ul> <p><b>Note:</b> Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.</p> <ul style="list-style-type: none"> <li>rule-description – Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).</li> </ul> |

### Usage Guidelines

Use this command to permit traffic between networks/hosts based on the protocol type selected in the access list. The following protocols are supported:

- IP
- ICMP
- ICP
- UDP
- PROTO (any Internet protocol other than TCP, UDP, and ICMP)

The last ACE in the access list is an implicit deny statement.

Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. The packet is allowed or denied based on the ACL configuration.

- Filtering on TCP or UDP allows you to specify port numbers as filtering criteria.
- Select ICMP to allow/deny packets. Selecting ICMP filters ICMP packets based on ICMP type and code.



#### Note

The log option is functional only for router ACL's. The log option displays an informational logging message about the packet matching the entry sent to the console.

### Examples

```

nx9500-6C8809(config-ip-acl-test)#permit ip 172.16.10.0/24 any log rule-precedence 750
nx9500-6C8809(config-ip-acl-test)#permit tcp 172.16.10.0/24 any log rule-precedence 800
nx9500-6C8809(config-ip-acl-test)#show context
ip access-list test
 permit ip 172.16.10.0/24 any log rule-precedence 750
 permit tcp 172.16.10.0/24 any log rule-precedence 800
nx9500-6C8809(config-ip-acl-test)#

```

### Related Commands

|       |                                                               |
|-------|---------------------------------------------------------------|
| no    | Removes a specified IP permit access rule                     |
| alias | Creates and configures aliases (network, VLAN, service, etc.) |

*no (ipv4-acl)*

Removes a deny, permit, or disable rule

**Supported in the following platforms:**

- Access Points — AP 6522, AP 6532, AP 6562, AP 7502, AP 7522, AP 7532, AP 7161, AP 81XX, AP 8232
- Wireless Controllers — RFS 4000, RFS 6000
- Service Platforms — NX 7500, NX 9500, NX 9510

**Syntax**

```
no [deny|disable|permit]
no [deny|permit] [<NETWORK-SERVICE-ALIAS-NAME>|icmp|ip|proto|tcp|udp]
 <RULE-PARAMETERS>
no disable [deny|permit] [<NETWORK-SERVICE-ALIAS-NAME>|icmp|ip|proto|tcp|udp]
 <RULE-PARAMETERS>
```

**Parameters**

```
no [deny|permit] <NETWORK-SERVICE-ALIAS-NAME>icmp|ip|proto|tcp|udp] <RULE-PARAMETERS>
```

|                                                     |                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| no [deny permit]                                    | Removes a deny or permit rule from the selected IP access list                                                                                                                                                                                                  |
| <NETWORK-SERVICE-ALIAS-NAME>                        | Removes a deny or permit rule applicable to the specified network-service alias <ul style="list-style-type: none"><li>• &lt;NETWORK-SERVICE-ALIAS-NAME&gt; - Specify the network-service alias name (should be associated with the deny/permit rule).</li></ul> |
| icmp                                                | Removes a deny or permit rule applicable to ICMP packets only                                                                                                                                                                                                   |
| ip                                                  | Removes a deny or permit rule applicable to IP packets only                                                                                                                                                                                                     |
| proto                                               | Removes a deny or permit rule applicable to protocols (other than IP, ICMP, TCP, and UDP)                                                                                                                                                                       |
| [tcp udp]                                           | Removes a deny or permit rule applicable to TCP/UDP packets                                                                                                                                                                                                     |
| <RULE-PARAMETERS>                                   | Enter the exact parameters used when configuring the rule.                                                                                                                                                                                                      |
| rule-precedence <1-5000><br>rule-description <LINE> | Specify the precedence assigned to this deny/permit rule. <ul style="list-style-type: none"><li>• rule-description - Optional. Specify the rule description.</li></ul> <p><b>Note:</b> The system removes the rule from the selected ACL.</p>                   |

```
no disable [deny|permit] [<NETWORK-SERVICE-ALIAS-NAME>|icmp|ip|proto|tcp|udp]
 <RULE-PARAMETERS>
```

|                              |                                                                                                                                                                                                                                                                          |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| no disabled [deny permit]    | Removes a disabled deny or permit rule from the selected IP access list                                                                                                                                                                                                  |
| <NETWORK-SERVICE-ALIAS-NAME> | Removes a disabled deny or permit rule applicable to the specified network-service alias <ul style="list-style-type: none"><li>• &lt;NETWORK-SERVICE-ALIAS-NAME&gt; - Specify the network-service alias name (should be associated with the deny/permit rule).</li></ul> |
| icmp                         | Removes a disabled deny or permit rule applicable to ICMP packets only                                                                                                                                                                                                   |
| ip                           | Removes a disabled deny or permit rule applicable to IP packets only                                                                                                                                                                                                     |
| proto                        | Removes a disabled deny or permit rule applicable to protocols (other than IP, ICMP, TCP, and UDP)                                                                                                                                                                       |
| [tcp udp]                    | Removes a disabled deny or permit rule applicable to TCP/UDP packets                                                                                                                                                                                                     |



|                                                     |                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <RULE-PARAMETERS>                                   | Enter the exact parameters used when configuring the rule.                                                                                                                                                                                                      |
| rule-precedence <1-5000><br>rule-description <LINE> | Specify the precedence assigned to this disabled deny/permit rule. <ul style="list-style-type: none"> <li>rule-description – Optional. Specify the rule description.</li> </ul> <p><b>Note:</b> The system removes the disabled rule from the selected ACL.</p> |

### Usage Guidelines

Provide the rule-precedence value when using the no command.

### Examples

The following example shows the ACL 'test' settings before the 'no' commands are executed:

```
<exsw1>(config-ip-acl-test)#show context
ip access-list test
 deny proto vrrp any any log rule-precedence 600
 deny proto ospf any any log rule-precedence 650
```

```
<exsw1>(config-ip-acl-test)#
<exsw1>(config-ip-acl-test)#no deny proto vrrp any any rule-precedence 600
<exsw1>(config-ip-acl-test)#no deny proto ospf any any rule-precedence 650
```

The following example shows the ACL 'test' settings after the 'no' commands are executed:

```
<exsw1>(config-ip-acl-test)#show context
ip access-list test
<exsw1>(config-ip-acl-test)#
```

### Related Commands

|         |                                                 |
|---------|-------------------------------------------------|
| deny    | Creates a deny access rule                      |
| disable | Disables a deny or permit rule within an IP ACL |
| permit  | Creates a permit access rule                    |

## mac-access-list

The following table summarizes MAC Access list configuration commands:

**Table 36: MAC-Access-List-Config Commands**

| Command | Description                                                                                                     |
|---------|-----------------------------------------------------------------------------------------------------------------|
| deny    | Creates a new deny access rule or modifies an existing rule. A deny access rule marks packets for rejection.    |
| disable | Disables a MAC deny or permit rule without removing it from the ACL                                             |
| ex3500  | Creates a MAC ACL deny and/or permit rule applicable only to the EX3500 switch                                  |
| insert  | Inserts a rule in an MAC ACL without overwriting or replacing an existing rule having the same precedence       |
| no      | Removes a deny and/or a permit access rule from a MAC ACL                                                       |
| permit  | Creates a new permit access rule or modifies an existing rule. A deny access rule marks packets for forwarding. |

## deny (mac-acl)

Creates a deny rule that marks packets (from a specified source MAC and/or to a specified destination MAC) for rejection. You can also use this command to modify an existing deny rule.



### Note

Use a decimal value representation to implement a permit/deny designation for a packet. The command set for MAC ACLs provide the hexadecimal values for each listed EtherType. Use the decimal equivalent of the EtherType listed for any other EtherType.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
deny [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <SOURCE-HOST-MAC>]
[<DEST-MAC> <DEST-MAC-MASK>|any|host <DEST-HOST-MAC>] (dot1p <0-7>,type [8021q|<1-65535>|
aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],vlan <1-4095>,log,rule-precedence <1-5000>)
{(rule-description <LINE>)}
```

### Parameters

```
deny [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <SOURCE-HOST-MAC>]
[<DEST-MAC> <DEST-MAC-MASK>|any|host <DEST-HOST-MAC>] (dot1p <0-7>,type [8021q|<1-65535>|
aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],vlan <1-4095>,log,rule-precedence <1-5000>)
{(rule-description <LINE>)}
```

|                                   |                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <SOURCE-MAC><br><SOURCE-MAC-MASK> | Configures the source MAC address and mask to match <ul style="list-style-type: none"><li>• &lt;SOURCE-MAC&gt; - Specify the source MAC address to match.</li><li>• &lt;SOURCE-MAC-MASK&gt; - Specify the source MAC address mask.</li></ul> Packets received from the specified MAC addresses are dropped.                    |
| any                               | Identifies all devices as the source to deny access. Packets received from any source are dropped.                                                                                                                                                                                                                             |
| host <SOURCE-HOST-MAC>            | Identifies a specific host as the source to deny access <ul style="list-style-type: none"><li>• &lt;SOURCE-HOST-MAC&gt; - Specify the source host's exact MAC address to match. Packets received from the specified host are dropped.</li></ul>                                                                                |
| <DEST-MAC><br><DEST-MAC-MASK>     | Configures the destination MAC address and mask to match <ul style="list-style-type: none"><li>• &lt;DEST-MAC&gt; - Specify the destination MAC address to match.</li><li>• &lt;DEST-MAC-MASK&gt; - Specify the destination MAC address mask to match.</li></ul> Packets addressed to the specified MAC addresses are dropped. |
| any                               | Identifies all devices as the destination to deny access. Packets addressed to any destination are dropped.                                                                                                                                                                                                                    |
| host <DEST-HOST-MAC>              | Identifies a specific host as the destination to deny access <ul style="list-style-type: none"><li>• &lt;DEST-HOST-MAC&gt; - Specify the destination host's exact MAC address to match. Packets addressed to the specified host are dropped.</li></ul>                                                                         |

|                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dot1p <0-7>                                                               | Configures the 802.1p priority value. Sets the service classes for traffic handling <ul style="list-style-type: none"> <li>• &lt;0-7&gt; – Specify 802.1p priority from 0 - 7.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| type [8021q <1-65535>  aarp  appletalk  ar ip  ipv6 ipx mint  rarp  wisp] | Configures the EtherType value<br>An EtherType is a two-octet field in an Ethernet frame that indicates the protocol encapsulated in the payload of the frame. The EtherType values are: <ul style="list-style-type: none"> <li>• 8021q – Indicates a 802.1q payload (0x8100)</li> <li>• &lt;1-65535&gt; – Indicates the EtherType protocol number</li> <li>• aarp – Indicates the Appletalk ARP payload (0x80F3)</li> <li>• appletalk – Indicates the Appletalk Protocol payload (0x809B)</li> <li>• ar – Indicates the ARP payload (0x0806)</li> <li>• ip – Indicates the Internet Protocol, Version 4 (IPv4) payload (0x0800)</li> <li>• ipv6 – Indicates the Internet Protocol, Version 6 (IPv6) payload (0x86DD)</li> <li>• ipx – Indicates the Novell's IPX payload (0x8137)</li> <li>• mint – Indicates the MiNT protocol payload (0x8783)</li> <li>• rarp – Indicates the reverse ARP payload (0x8035)</li> <li>• wisp – Indicates the WIPS (Wireless Internet Service Provider) payload (0x8783)</li> </ul> |
| vlan <1-4095>                                                             | Configures the VLAN where the traffic is received <ul style="list-style-type: none"> <li>• &lt;1-4095&gt; – Specify the VLAN ID from 1 - 4095.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| log                                                                       | Logs all deny events matching this entry. If a source and/or destination MAC address is matched (i.e., a packet is received from a specified MAC address or is destined for a specified MAC address), an event is logged.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| rule-precedence <1-5000> rule-description <LINE>                          | The following keywords are recursive and common to all of the above parameters: <ul style="list-style-type: none"> <li>• rule-precedence – Assigns a precedence for this deny rule <ul style="list-style-type: none"> <li>• &lt;1-5000&gt; – Specify a value from 1 - 5000.</li> </ul> <p><b>Note:</b> Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.</p> </li> <li>• rule-description – Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                |

### Usage Guidelines

The deny command disallows traffic based on layer 2 (data-link layer) data. The MAC access list denies traffic from a particular source MAC address or any MAC address. It can also disallow traffic from a list of MAC addresses based on the source mask.

The MAC access list can disallow traffic based on the VLAN and EtherType.

- ARP
- WISP
- IP
- 802.1q



#### Note

MAC ACLs always takes precedence over IP based ACLs.

The last ACE in the access list is an implicit deny statement. Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. It is allowed or denied based on the ACL's configuration.

### Examples

```
rfs4000-229D58(config-mac-acl-test)#deny 41-85-45-89-66-77 ff-ff-ff-00-00-00 any
vlan 1 rule-precedence 1
rfs4000-229D58(config-mac-acl-test)#deny host 00-01-ae-00-22-11 any rule-precedence 2
rfs4000-229D58(config-mac-acl-test)#show context
mac access-list test
 deny 41-85-45-89-66-77 FF-FF-FF-00-00-00 any vlan 1 rule-precedence 1
 deny host 00-01-AE-00-22-11 any rule-precedence 2
rfs4000-229D58(config-mac-acl-test)#
```

The MAC ACL (in the example below) denies traffic from any source MAC address to a particular host MAC address:

```
nx9500-6C8809(config-mac-acl-test)#deny any host 00:01:ae:00:22:11 vlan 1 log rule-
precedence 1
```

The following example denies traffic between two hosts based on MAC addresses:

```
nx9500-6C8809(config-mac-acl-test)#deny host 01:02:fe:45:76:89 host 01:02:89:78:78:45 vlan
1 log rule-precedence 1
```

### Related Commands

|           |                                          |
|-----------|------------------------------------------|
| <b>no</b> | Removes a specified MAC deny access rule |
|-----------|------------------------------------------|

### *disable (mac-acl)*

Disables a MAC deny or permit rule without removing it from the ACL. A disabled rule is inactive and is not used to filter packets.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
disable [deny|insert|permit]
disable [deny|permit] [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <SOURCE-HOST-MAC>]
[<DEST-MAC> <DEST-MAC-MASK>|any|host <DEST-HOST-MAC>] (dot1p <0-7>|mark [8021p <0-7>|dscp
<0-63>],
type [8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],vlan <1-4095>) log
(rule-precedence <1-5000>) {(rule-description <LINE>)}
disable insert [deny|permit]
```

### Parameters

```
disable [deny|permit] [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <SOURCE-HOST-MAC>]
[<DEST-MAC> <DEST-MAC-MASK>|any|host <DEST-HOST-MAC>] (dot1p <0-7>|mark [8021p <0-7>|dscp
<0-63>],
type [8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],vlan <1-4095>) log
(rule-precedence <1-5000>) {(rule-description <LINE>)}
```

|                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| disable [deny insert permit]                                          | Disables a deny, insert or permit access rule without removing it from the MAC ACL<br>Provide the exact values used to configure the deny or permit rule that is to be disabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <SOURCE-MAC> <SOURCE-MAC-MASK>                                        | Specifies the source MAC address and mask to match <ul style="list-style-type: none"> <li>&lt;SOURCE-MAC&gt; - Specify the source MAC address to match.</li> <li>&lt;SOURCE-MAC-MASK&gt; - Specify the source MAC address mask.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                            |
| any                                                                   | Select 'any' if the rule is applicable to any source MAC address                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| host <SOURCE-HOST-MAC>                                                | Specify the source host's exact MAC address                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <DEST-MAC> <DEST-MAC-MASK>                                            | Specifies the destination MAC address and mask to match <ul style="list-style-type: none"> <li>&lt;DEST-MAC&gt; - Specify the destination MAC address.</li> <li>&lt;DEST-MAC-MASK&gt; - Specify the destination MAC address mask.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                          |
| any                                                                   | Select 'any' if the rule is applicable to any destination MAC address                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| host <DEST-HOST-MAC>                                                  | Specify the destination host's exact MAC address                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| log                                                                   | The following keyword defines the action taken when a packet matches any of the deny rules: <ul style="list-style-type: none"> <li>log - Logs a record, when a packet matches the specified criteria</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                       |
| dot1p <0-7>                                                           | Specify the 802.1p priority from 0 - 7.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| mark [8021p <0-7>,dscp <0-63>]                                        | Marks/modifies packets that match the criteria specified here <ul style="list-style-type: none"> <li>8021p &lt;0-7&gt; - Modifies 802.1p VLAN user priority from 0 - 7</li> <li>dscp &lt;0-63&gt; - Modifies DSCP TOS bits in the IP header from 0 - 63</li> </ul> <p><b>Note:</b> This option is applicable only to the MAC ACL permit rule.</p>                                                                                                                                                                                                                                                                                     |
| type [8021q <1-65535> arp appletalk  arplip ipv6 ipx mint  rarp wisp] | Use the available options to specify the EtherType value to match.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| vlan <1-4095>                                                         | Specify the VLAN ID(s)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| log                                                                   | Select log, if the rule has been configured to log records in case of a match.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| rule-precedence <1-5000> {(rule-description <LINE>)}                  | The following keywords are recursive and common to all of the above parameters: <ul style="list-style-type: none"> <li>rule-precedence - Assigns a precedence for this rule <ul style="list-style-type: none"> <li>&lt;1-5000&gt; - Specify a value from 1 - 5000.</li> </ul> <p><b>Note:</b> Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.</p> </li> <li>rule-description - Optional. Configures a description for this rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).</li> </ul> |

## Examples

The following example shows the MAC access list 'test' settings before the 'disable' command is executed:

```
rfs4000-229D58(config-mac-acl-test)#show context
mac access-list test
deny 41-85-45-89-66-77 FF-FF-FF-00-00-00 any vlan 1 rule-precedence 1
```

```
deny host 00-01-AE-00-22-11 any rule-precedence 2
rfs4000-229D58(config-mac-acl-test)#
rfs4000-229D58(config-mac-acl-test)#disable deny host 00-01-AE-00-22-11 any rule-
precedence 2
```

The following example shows the MAC access list 'test' settings after the 'disable' command is executed:

```
rfs4000-229D58(config-mac-acl-test)#show context
mac access-list test
deny 41-85-45-89-66-77 FF-FF-FF-00-00-00 any vlan 1 rule-precedence 1
disable deny host 00-01-AE-00-22-11 any rule-precedence 2
rfs4000-229D58(config-mac-acl-test)#
```

## Related Commands

|           |                                        |
|-----------|----------------------------------------|
| <b>no</b> | Enables a disabled deny or permit rule |
|-----------|----------------------------------------|

### ex3500 (mac-acl-config-commands)

Creates a MAC ACL deny and/or permit rule, applicable only to the EX3500 switch

Each deny or permit rule consists of a set of match criteria and an associated action, which is deny access for the deny rule and allow access for the permit rule. When applied to layer 2 traffic (between a EX35XX switch and the WiNG managed service platform or a WiNG VM interface) every packet is matched against the configured match criteria and in case of a match the packet is dropped or forwarded depending on the rule type.

EX35XX devices (EX3524 and EX3548) are layer 2 Gigabit Ethernet switches with either 24 or 48 10/100/1000-BASE-T ports, and four SFP transceiver slots for fiber connectivity. Each 10/100/1000 Mbps port supports both the IEEE 802.3af and IEEE 802.3at-2009 PoE standards. An EX35XX switch has an SNMP-based management agent that provides both in-band and out-of-band management access. The EX35XX switch utilizes an embedded HTTP Web agent and CLI, which in spite of being different from that of the WiNG operating system provides WiNG controllers PoE and port management resources.



#### Note

To implement the EX3500 MAC ACL rule, apply the MAC ACL directly to a EX35XXwi device, or to an EX35XX profile. For more information, see [access-group](#) on page 1299.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
ex3500 [deny|permit] [all|tagged-eth2|untagged-eth2]
ex3500 [deny|permit] [all|tagged-eth2|untagged-eth2] [any |host <SOURCE-MAC>|
network <SOURCE-MAC> <SOURCE-MAC-MASK>] [any|host <DEST-MAC>|network <DEST-MAC>
<DEST-MAC-MASK>] [ethertype <0-65535>|ethertype-mask <0-65535>|ex3500-time-range
<TIME-RANGE-NAME>|rule-precedence <1-128>|vlan <1-4094>|vlan-mask <1-4095>]
```

## Parameters

```
ex3500 [deny|permit] [all|tagged-eth2|untagged-eth2] [any |host <SOURCE-MAC>|
network <SOURCE-MAC> <SOURCE-MAC-MASK>] [any|host <DEST-MAC>|network <DEST-MAC>
<DEST-MAC-MASK>] [ethertype <0-65535|ethertype-mask <0-65535>|ex3500-time-range
<TIME-RANGE-NAME>|rule-precedence <1-128>|vlan <1-4094>|vlan-mask <1-4095>]
```

|                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [deny permit]                                                    | <p>Creates a deny or permit MAC ACL rule and configures the rule parameters. Every EX3500 MAC ACL rule provides a set of match criteria against which incoming and outgoing packets (to and from an EX35XX device) are matched. In case of a match, the packet is dropped or forwarded depending on the rule type. The packet is dropped in case of a deny rule, and forwarded for an permit rule.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| [all tagged-eth2  untagged-eth2]                                 | <p>Specifies the packet type</p> <ul style="list-style-type: none"> <li>all - Applies this deny/permit rule to all packets</li> <li>tagged-eth2 - Applies this deny/permit rule only to tagged Ethernet-2 packets</li> <li>untagged-eth2 - Applies this deny/permit rule only to untagged Ethernet-2 packets</li> </ul> <p>After specifying the packet type, configure the source and/or EX3500 MAC addresses to match.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| [any] host <SOURCE-MAC>  network <SOURCE-MAC> <SOURCE-MAC-MASK>] | <p>Enter the Source MAC addresses</p> <ul style="list-style-type: none"> <li>any - Identifies all EX3500 devices as a source to match</li> <li>host &lt;SOURCE-MAC&gt; - Identifies a specific EX3500 host as the source to match <ul style="list-style-type: none"> <li>&lt;SOURCE-MAC&gt; - Specify the source host's exact MAC address</li> </ul> </li> <li>network &lt;SOURCE-MAC&gt; &lt;SOURCE-MAC-MASK&gt; - Configures a range of MAC addresses as the source to match. Packets received from any of these MAC addresses are dropped. <ul style="list-style-type: none"> <li>&lt;SOURCE-MAC&gt; - Specify the source MAC address to match.</li> <li>&lt;SOURCE-MAC-MASK&gt; - Specify the source MAC bit mask.</li> </ul> </li> </ul> <p>For a deny rule, packets received from EX3500 device(s) matching the specified MAC address(es) are dropped.<br/>For a permit rule, packets received from EX3500 device(s) matching the specified MAC address(es) are forwarded.</p>                                 |
| [any host <DEST-MAC>  network <DEST-MAC> <DEST-MAC-MASK>]        | <p>Enter the Destination MAC addresses</p> <ul style="list-style-type: none"> <li>any - Identifies all EX3500 devices as a destination to match</li> <li>host &lt;SOURCE-MAC&gt; - Identifies a specific EX3500 host as the destination to match <ul style="list-style-type: none"> <li>&lt;SOURCE-MAC&gt; - Specify the destination host's exact MAC address</li> </ul> </li> <li>network &lt;SOURCE-MAC&gt; &lt;SOURCE-MAC-MASK&gt; - Configures a range of MAC addresses as the destination to match. Packets addressed to any of these MAC addresses are dropped. <ul style="list-style-type: none"> <li>&lt;SOURCE-MAC&gt; - Specify the destination MAC address to match.</li> <li>&lt;SOURCE-MAC-MASK&gt; - Specify the destination MAC bit mask.</li> </ul> </li> </ul> <p>For a deny rule, packets addressed to EX3500 device(s) matching the specified MAC address(es) are dropped.<br/>For a permit rule, packets addressed to EX3500 device(s) matching the specified MAC address(es) are forwarded.</p> |

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ether-type <0-65535>                | Configures the EtherType protocol number. The ether type is a two-octet field within an Ethernet frame. It indicates the protocol encapsulated in the payload of an Ethernet frame. <ul style="list-style-type: none"> <li>&lt;0-65535&gt; - Specify the value from 0 - 65535. The default value is 1.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| ethertype-mask <0-65535>            | Configures the EtherType mask <ul style="list-style-type: none"> <li>&lt;0-65535&gt; - Specify the value from 0 - 65535. The default value is 1.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| ex3500-time-range <TIME-RANGE-NAME> | Applies a specified EX3500 time range (should be existing and configured). The deny or permit rule is applied during the time period specified in the EX3500 time range. <ul style="list-style-type: none"> <li>&lt;TIME-RANGE-NAME&gt; - Specify the time range name.</li> </ul> <p>An EX3500 time range list consists of a set of periodic and absolute time range rules. Periodic time ranges recur periodically at specified time periods, such as daily, weekly, weekends, weekdays, and on specific week days, for example on every successive Mondays. Absolute time ranges are not periodic and do not recur. They consist of a range of days during a particular time period (the starting and ending days and time are fixed).</p> <p><b>Note:</b> For information on configuring EX3500 time-range, see <a href="#">ex3500</a>.</p> |
| vlan <1-4094>                       | Configures a VLAN ID representative of the shared SSID each user employs to interoperate within the network (once authenticated by the local RADIUS server) <ul style="list-style-type: none"> <li>&lt;1-4094&gt; - Specify the VLAN ID from 1 - 4094.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| vlan-mask <1-4095>                  | Configures the VLAN ID bit mask value <ul style="list-style-type: none"> <li>&lt;1-4095&gt; - Specify the VLAN bit mask from 1 - 4095.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| rule-precedence <1-128>             | Configures a precedence for this EX3500 MAC ACL <ul style="list-style-type: none"> <li>&lt;1 - 128&gt; - Specify a value from 1 - 128. ACLs with lower precedence are applied first to packets.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## Examples

```

nx9500-6C8809(config-mac-acl-ex3500MacACL)#ex3500 deny tagged-eth2 any any vlan
20 rule-precedence 1
nx9500-6C8809(config-mac-acl-ex3500MacACL)#show context
mac access-list ex3500MacACL
 ex3500 deny tagged-eth2 any any vlan 20 rule-precedence 1
nx9500-6C8809(config-mac-acl-ex3500MacACL)#

```

## Related Commands

|                                           |                                                       |
|-------------------------------------------|-------------------------------------------------------|
| <a href="#">no (mac-acl)</a> on page 1401 | Removes this EX3500 deny/permit rule from the MAC ACL |
|-------------------------------------------|-------------------------------------------------------|

### *insert (mac-acl)*

Enables the insertion of a rule in an MAC ACL without overwriting or replacing an existing rule having the same precedence

The insert option allows a new rule to be inserted within a MAC ACL. Consider an MAC ACL consisting of rules having precedences 1, 2, 3, 4, 5, and 6. You want to insert a new rule with precedence 4, without overwriting the existing precedence 4 rule. Using the insert option inserts the new rule prior to the



existing one. The existing precedence 4 rule's precedence changes to 5, and the change cascades down the list of rules within the ACL. That means rule 5 becomes rule 6, and rule 6 becomes rule 7.



#### Note

NOT using insert when creating a new rule having the same precedence as an existing rule, overwrites the existing rule.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
insert [deny|permit] <PARAMETERS> (dot1p <0-7>,mark [8021p <0-7>|dscp <0-63>],
type [8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],vlan <1-4095>,
log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

#### Parameters

```
insert [deny|permit] <PARAMETERS> (dot1p <0-7>,mark [8021p <0-7>|dscp <0-63>],
type [8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],vlan <1-4095>,
log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

|                                |                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| insert [deny permit]           | Inserts a deny or permit rule within an MAC ACL                                                                                                                                                                                                                                                                                                    |
| <PARAMETERS>                   | Provide the match criteria for this deny/permit rule. Packets will be filtered based on the criteria set here.<br>For more information on the deny rule, see <a href="#">deny</a> .<br>For more information on the permit rule, see <a href="#">permit</a> .                                                                                       |
| dot1p <0-7>                    | Configures the 802.1p priority value. Sets the service classes for traffic handling <ul style="list-style-type: none"><li>• &lt;0-7&gt; - Specify 802.1p priority from 0 - 7.</li></ul>                                                                                                                                                            |
| mark [8021p <0-7>,dscp <0-63>] | Marks/modifies packets that match the criteria specified here <ul style="list-style-type: none"><li>• 8021p &lt;0-7&gt; - Modifies 802.1p VLAN user priority from 0 - 7</li><li>• dscp &lt;0-63&gt; - Modifies DSCP TOS bits in the IP header from 0 - 63</li></ul> <p><b>Note:</b> This option is applicable only to the MAC ACL permit rule.</p> |

|                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| type [8021q <1-65535>  aarp  appletalk  arpl ip ipv6  ipx mint  rarp wisp] | Configures the EtherType value<br>An EtherType is a two-octet field in an Ethernet frame that indicates the protocol encapsulated in the payload of the frame. The EtherType values are: <ul style="list-style-type: none"> <li>• 8021q - Indicates a 802.1q payload (0x8100)</li> <li>• &lt;1-65535&gt; - Indicates the EtherType protocol number</li> <li>• aarp - Indicates the Appletalk ARP payload (0x80F3)</li> <li>• appletalk - Indicates the Appletalk Protocol payload (0x809B)</li> <li>• arp - Indicates the ARP payload (0x0806)</li> <li>• ip - Indicates the IPv4 payload (0x0800)</li> <li>• ipv6 - Indicates the IPv6 payload (0x86DD)</li> <li>• ipx - Indicates the Novell's IPX payload (0x8137)</li> <li>• mint - Indicates the MiNT protocol payload (0x8783)</li> <li>• rarp - Indicates the reverse ARP payload (0x8035)</li> <li>• wisp - Indicates the WISP payload (0x8783)</li> </ul> |
| vlan <1-4095>                                                              | Configures the VLAN where the traffic is received <ul style="list-style-type: none"> <li>• &lt;1-4095&gt; - Specify the VLAN ID from 1 - 4095.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| log                                                                        | Logs all deny/permit events matching this entry. If a source and/or destination MAC address is matched (i.e. a packet is received from a specified MAC address or is destined for a specified MAC address), an event is logged.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| rule-precedence <1-5000> rule-description <LINE>                           | The following keywords are recursive and common to all of the above parameters: <ul style="list-style-type: none"> <li>• rule-precedence - Assigns a precedence for this deny/permit rule</li> <li>• &lt;1-5000&gt; - Specify a value from 1 - 5000.</li> </ul> <p><b>Note:</b> Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.</p> <ul style="list-style-type: none"> <li>• rule-description - Optional. Configures a description for this deny/permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).</li> </ul>                                                                                                                                                                                                                                                 |

## Examples

```
rfs4000-229D58(config-mac-acl-test1)#deny 11-22-33-44-55-66 11-22-33-44-55-77 any rule-
precedence 1
rfs4000-229D58(config-mac-acl-test1)#deny host B4-C7-99-6D-CD-9B any rule-precedence 2
rfs4000-229D58(config-mac-acl-test1)#show context
mac access-list test1
 deny 11-22-33-44-55-66 11-22-33-44-55-77 any rule-precedence 1
 deny host B4-C7-99-6D-CD-9B any rule-precedence 2
rfs4000-229D58(config-mac-acl-test1)#
```

In the following example a new rule is inserted between the rules having precedences 1 and 2. The precedence of the existing precedence '2' rule changes to precedence 3.

```
rfs4000-229D58(config-mac-acl-test1)#insert permit host B4-C7-99-6D-B5-D6 host B4-C7-99-6D-
CD-9B rule-precedence 2
rfs4000-229D58(config-mac-acl-test1)#show context
mac access-list test1
 deny 11-22-33-44-55-66 11-22-33-44-55-77 any rule-precedence 1
 permit host B4-C7-99-6D-B5-D6 host B4-C7-99-6D-CD-9B rule-precedence 2
 deny host B4-C7-99-6D-CD-9B any rule-precedence 3
rfs4000-229D58(config-mac-acl-test1)#
```

## permit (mac-acl)

Creates a permit rule that marks packets (from a specified source MAC and/or to a specified destination MAC) for forwarding. You can also use this command to modify an existing permit rule.



### Note

Use a decimal value representation to implement a permit/deny designation for a packet. The command set for MAC ACLs provide the hexadecimal values for each listed EtherType. Use the decimal equivalent of the EtherType listed for any other EtherType.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
permit [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <SOURCE-HOST-MAC>] [<DEST-MAC> <DEST-MAC-MASK>|any|host <DEST-HOST-MAC>] (dot1p <0-7>,mark [8021p <0-7>,dscp <0-63>],type [8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],vlan <1-4095>) log (rule-precedence <1-5000>){(rule-description <LINE>)}
```

### Parameters

```
permit [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <SOURCE-HOST-MAC>] [<DEST-MAC> <DEST-MAC-MASK>|any|host <DEST-HOST-MAC>] (dot1p <0-7>,mark [8021p <0-7>,dscp <0-63>],type [8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],vlan <1-4095>) log (rule-precedence <1-5000>){(rule-description <LINE>)}
```

|                                   |                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <SOURCE-MAC><br><SOURCE-MAC-MASK> | Configures the source MAC address and mask to match <ul style="list-style-type: none"><li>• &lt;SOURCE-MAC&gt; - Specify the source MAC address to match.</li><li>• &lt;SOURCE-MAC-MASK&gt; - Specify the source MAC address mask.</li></ul> Packets addressed to the specified MAC addresses are forwarded.                     |
| any                               | Identifies all devices as the source to permit access. Packets received from any source are forwarded.                                                                                                                                                                                                                           |
| host <SOURCE-HOST-MAC>            | Identifies a specific host as the source to permit access <ul style="list-style-type: none"><li>• &lt;SOURCE-HOST-MAC&gt; - Specify the source host's exact MAC address to match.</li></ul> Packets received from the specified host are forwarded.                                                                              |
| <DEST-MAC><br><DEST-MAC-MASK>     | Configures the destination MAC address and mask to match <ul style="list-style-type: none"><li>• &lt;DEST-MAC&gt; - Specify the destination MAC address to match.</li><li>• &lt;DEST-MAC-MASK&gt; - Specify the destination MAC address mask to match.</li></ul> Packets addressed to the specified MAC addresses are forwarded. |
| any                               | Identifies all devices as the destination to permit access. Packets addressed to any destination are forwarded.                                                                                                                                                                                                                  |

|                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| host <DEST-HOST-MAC>                                                       | Identifies a specific host as the destination to permit access <ul style="list-style-type: none"> <li>• &lt;DEST-HOST-MAC&gt; – Specify the destination host’s exact MAC address to match. Packets addressed to the specified host are forwarded.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| dot1p <0-7>                                                                | Configures the 802.1p priority value. Sets the service classes for traffic handling <ul style="list-style-type: none"> <li>• &lt;0-7&gt; – Specify 802.1p priority from 0 - 7.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| type [8021q <1-65535>  aarp  appletalk  arplip  ipv6 ipx mint  rarp  wisp] | Configures the EtherType value<br>An EtherType is a two-octet field in an Ethernet frame that indicates the protocol encapsulated in the payload of the frame. The EtherType values are: <ul style="list-style-type: none"> <li>• 8021q – Indicates a 802.1q payload (0x8100)</li> <li>• &lt;1-65535&gt; – Indicates the EtherType protocol number</li> <li>• aarp – Indicates the Appletalk ARP payload (0x80F3)</li> <li>• appletalk – Indicates the Appletalk Protocol payload (0x809B)</li> <li>• arp – Indicates the ARP payload (0x0806)</li> <li>• ip – Indicates the IPv4 payload (0x0800)</li> <li>• ipv6 – Indicates the IPv6 payload (0x86DD)</li> <li>• ipx – Indicates the Novell’s IPX payload (0x8137)</li> <li>• mint – Indicates the MiNT protocol payload (0x8783)</li> <li>• rarp – Indicates the reverse ARP payload (0x8035)</li> <li>• wisp – Indicates the WISP payload (0x8783)</li> </ul> |
| vlan <1-4095>                                                              | Configures the VLAN ID <ul style="list-style-type: none"> <li>• &lt;1-4095&gt; – Specify the VLAN ID from 1 - 4095.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| log                                                                        | Logs all permit events matching this entry. If a source and/or destination MAC address is matched (i.e. a packet is addressed to a specified MAC address or is destined for a specified MAC address), an event is logged.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| rule-precedence <1-5000> rule-description <LINE>                           | The following keywords are recursive and common to all of the above parameters: <ul style="list-style-type: none"> <li>• rule-precedence – Assigns a precedence for this permit rule <ul style="list-style-type: none"> <li>• &lt;1-5000&gt; – Specify a value from 1 - 5000.</li> </ul> <p><b>Note:</b> Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.</p> </li> <li>• rule-description – Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).</li> </ul>                                                                                                                                                                                                                                                          |

### Usage Guidelines

The permit command in the MAC ACL allows traffic based on layer 2 (data-link layer) information. A MAC access list permits traffic from a source MAC address or any MAC address. It also has an option to allow traffic from a list of MAC addresses (based on the source mask).

The MAC access list can be configured to allow traffic based on VLAN information, or Ethernet type. Common types include:

- ARP
- WISP
- IP
- 802.1q

Layer 2 traffic is not allowed by default. To adopt an Access Point through an interface, configure an ACL to allow an Ethernet WISP.

Use the mark option to specify the ToS (type of service) and priority value. The tos value is marked in the IP header and the 802.1p priority value is marked in the dot1q frame.

Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. It is marked based on the ACL's configuration.



#### Note

To apply an IP based ACL to an interface, a MAC access list entry is mandatory to allow ARP. A MAC ACL always takes precedence over IP based ACLs.

### Examples

```
nx9500-6C8809(config-mac-acl-test)#permit host 11-22-33-44-55-66 any log mark 8021p 3 rule-
precedence 600
nx9500-6C8809(config-mac-acl-test)#permit host 22-33-44-55-66-77 host 11-22-33-44-55-66
type ip log rule-precedence 610
nx9500-6C8809(config-mac-acl-test)#show context
mac access-list test
 permit host 11-22-33-44-55-66 any log mark 8021p 3 rule-precedence 600
 permit host 22-33-44-55-66-77 host 11-22-33-44-55-66 type ip log rule-precedence 610
nx9500-6C8809(config-mac-acl-test)#
```

### Related Commands

|                 |                                                   |
|-----------------|---------------------------------------------------|
| <code>no</code> | Removes or resets a specified MAC ACL permit rule |
|-----------------|---------------------------------------------------|

*no (mac-acl)*

Negates a command or sets its default

### Supported in the following platforms:

- Access Points — AP 6522, AP 6532, AP 6562, AP 7502, AP 7522, AP 7532, AP 7161, AP 81XX, AP 8232
- Wireless Controllers — RFS 4000, RFS 6000
- Service Platforms — NX 7500, NX 9500, NX 9510

### Syntax

```
no [deny|disable|permit]
no [deny|permit] [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <SOURCE-HOST-MAC>]
 [<DEST-MAC> <DEST-MAC-MASK>|any|host <DEST-HOST-MAC>] (dot1p <0-7>,type [8021q|<1-65535>|
 aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],vlan <1-4095>) log (rule-precedence
 <1-5000>)
 {(rule-description <LINE>)}

no disable [deny|permit] <RULE-PARAMETERS>
```

### Parameters

```
no [deny|permit] [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <SOURCE-HOST-MAC>]
 [<DEST-MAC> <DEST-MAC-MASK>|any|host <DEST-HOST-MAC>] (dot1p <0-7>,type [8021q|<1-65535>|
 aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],vlan <1-4095>) log (rule-precedence
 <1-5000>)
 {(rule-description <LINE>)}
```

|                                                                               |                                                                                                                                                                                                                        |
|-------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| no [deny permit]                                                              | Removes a deny or permit rule from the MAC ACL                                                                                                                                                                         |
| <SOURCE-MAC> <SOURCE-MAC-MASK>                                                | Specify the source MAC address and mask                                                                                                                                                                                |
| any                                                                           | Select 'any' if the rule is applicable to any source MAC address                                                                                                                                                       |
| host <SOURCE-HOST-MAC>                                                        | Specify the source host's exact MAC address.                                                                                                                                                                           |
| <DEST-MAC> <DEST-MAC-MASK>                                                    | Specify the destination MAC address and mask                                                                                                                                                                           |
| any                                                                           | Identifies all devices as the destination to deny/permit access                                                                                                                                                        |
| host <DEST-HOST-MAC>                                                          | Specify the destination host's exact MAC address.                                                                                                                                                                      |
| dot1p <0-7>                                                                   | Specify the 802.1p priority value from 0 -7.                                                                                                                                                                           |
| type [8021q <1-65535>  aarp <br>appletalk arp ip ipv6 ipx mint <br>rarp wisp] | Specify the EtherType value.                                                                                                                                                                                           |
| vlan <1-4095>                                                                 | Specify the VLAN ID.                                                                                                                                                                                                   |
| log                                                                           | Select log, if the rule has been configured to log records in case of a match.                                                                                                                                         |
| mark [8021p <0-7>  dscp <0-63>]                                               | This is specific to the MAC ACL permit rule. Marks packets that match the ACL rule<br>8021p <0-7> - Modifies 802.1p VLAN user priority from 0 - 7<br>dscp <0-63> - Modifies DSCP TOS bits in the IP header from 0 - 63 |
| rule-precedence <1-5000>                                                      | Specify the rule precedence. The rule with the specified rule precedence is removed from the MAC ACL.                                                                                                                  |
| rule-description <LINE>                                                       | Optional. Provide the description configured for the rule.                                                                                                                                                             |

no disable [deny|permit] <RULE-PARAMETERS>

|                                                       |                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| no disable [deny permit]                              | Removes a disabled deny or permit rule from the selected IP access list                                                                                                                                                                                         |
| <RULE-PARAMETERS>                                     | Enter the exact parameters used when configuring the rule.                                                                                                                                                                                                      |
| rule-precedence <1-5000> rule-<br>description <LINE>} | Specify the precedence assigned to this disabled deny/permit rule. <ul style="list-style-type: none"> <li>rule-description - Optional. Specify the rule description.</li> </ul> <p><b>Note:</b> The system removes the disabled rule from the selected ACL.</p> |

## Examples

```
<exsw1>(config-mac-acl-test)#show context
mac access-list test
 permit host 11-22-33-44-55-66 any log mark 8021p 3 rule-precedence 600
 permit host 22-33-44-55-66-77 host 11-22-33-44-55-66 type ip log rule-precedence 610
 deny any host 33-44-55-66-77-88 log rule-precedence 700

<exsw1>(config-mac-acl-test)#no deny any host 33-44-55-66-77-88 log rule-precedence 700
<exsw1>(config-mac-acl-test)#show context
mac access-list test
 permit host 11-22-33-44-55-66 any log mark 8021p 3 rule-precedence 600
 permit host 22-33-44-55-66-77 host 11-22-33-44-55-66 type ip log rule-precedence 610
```

## Related Commands

|        |                          |
|--------|--------------------------|
| deny   | Creates a MAC deny ACL   |
| permit | Creates a MAC permit ACL |

## ipv6-access-list

Configures an IPv6 ACL. IPv6 ACLs define a set of rules that filter IPv6 packets flowing through a port or interface. Each rule specifies the action taken when a packet matches the rule. If the action is deny, the packet is dropped. If the action is permit, the packet is allowed.

The WiNG software supports IPv6 only on VLAN interfaces. Therefore, IPv6 ACLs can be applied only on the VLAN interface.

The following table summarizes IPv6 access list configuration commands:

**Table 37: IPv6 Access List Config Mode Commands**

| Command                                     | Description                                                                                                                                                                |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>deny (ipv6-acl)</code> on page 1403   | Creates a deny access rule or modifies an existing rule. A deny access rule rejects IPv6 packets from specified address(es) and/or destined for specified address(es).     |
| <code>permit (ipv6-acl)</code> on page 1409 | Creates a permit access rule or modifies an existing rule. A permit access rule accepts IPv6 packets from specified address(es) and/or destined for specified address(es). |
| <code>no (ipv6-acl)</code> on page 1414     | Removes a deny and/or a access rule from a IPv6 ACL                                                                                                                        |

### *deny (ipv6-acl)*

Creates a deny rule that rejects packets from a specified IPv6 source and/or to a specified IPv6 destination. You can also use this command to modify an existing deny rule.

#### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### **Syntax**

```
deny [icmpv6|ipv6|proto|tcp|udp]
deny icmpv6 [<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/MASK>|any|
host <DEST-HOST-IPv6>] [code [eq <ICMPv6-CODE>|range <STARTING-ICMPv6-CODE> <ENDING-ICMPv6-
CODE>]]
type [eq <ICMPv6-TYPE>|range <STARTING-ICMPv6-TYPE> <ENDING-ICMPv6-TYPE>]]
(log,rule-precedence <1-5000>) {(rule-description <LINE>)}
deny ipv6 [<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/MASK>|any|
host <DEST-HOST-IPv6>] (log,rule-precedence <1-5000>) {(rule-description <LINE>)}
deny proto [<PROTOCOL-NUMBER>|<PROTOCOL-NAME>|eigrp|gre|igmp|ospf|vrrp]
[<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/MASK>|any|host <DEST-HOST-
IPv6>]
(log,rule-precedence <1-5000>) {(rule-description <LINE>)}
deny [tcp|udp] [<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/MASK>|any|
eq <SOURCE-PORT>|host <DEST-HOST-IPv6>|range <START-PORT> <END-PORT>] [eq [<1-65535>|<
SERVICE-NAME>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|ntp|pop3|sip|smtp|ssh|telnet|
tftp|www]]
range <START-PORT> <END-PORT>] (log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

## Parameters

```
deny icmpv6 [<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/MASK>|any|
host <DEST-HOST-IPv6>] [code [eq <ICMPv6-CODE>|range <STARTING-ICMPv6-CODE> <ENDING-ICMPv6-
CODE>]]
type [eq <ICMPv6-TYPE>|range <STARTING-ICMPv6-TYPE> <ENDING-ICMPv6-TYPE>]]
(log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

|                          |                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| icmpv6                   | Applies this deny rule to ICMPv6 packets only                                                                                                                                                                                                                                                                                                                                   |
| <SOURCE-IPv6/MASK>       | Specifies a range of IPv6 source address (network) to match. ICMPv6 packets received from any source in the specified network are dropped.                                                                                                                                                                                                                                      |
| any                      | Specifies the source as any IPv6 address. ICMPv6 packets received from any source are dropped.                                                                                                                                                                                                                                                                                  |
| host <SOURCE-HOST-IPv6>  | Identifies a specific host (as the source to match) by its IPv6 address. ICMPv6 packets received from the specified host are dropped. <ul style="list-style-type: none"> <li>&lt;SOURCE-HOST-IPv6&gt; - Specify the source host's exact IPv6 address.</li> </ul>                                                                                                                |
| <DEST-IPv6/MASK>         | Specifies a range of IPv6 destination address (network) to match. ICMPv6 packets addressed to any destination within the specified network are dropped.                                                                                                                                                                                                                         |
| any                      | Specifies the destination as any IPv6 address. ICMPv6 packets addressed to any destination are dropped.                                                                                                                                                                                                                                                                         |
| host <DEST-HOST-IPv6>    | Identifies a specific host (as the destination to match) by its IPv6 address. ICMPv6 packets addressed to the specified host are dropped. <ul style="list-style-type: none"> <li>&lt;DEST-HOST-IPv6&gt; - Specify the destination host's exact IPv6 address.</li> </ul>                                                                                                         |
| <ICMPv6-TYPE> [eq range] | Defines the ICMPv6 type field filter <ul style="list-style-type: none"> <li>eq - Configures a specific ICMPv6 type. Specify the ICMPv6 type value.</li> <li>range - Configures a range of ICMPv6 types. Specify the starting and ending ICMPv6 type values.</li> </ul> <p><b>Note:</b> ICMPv6 packets with type field value matching the values specified here are dropped.</p> |
| <ICMPv6-CODE>            | Defines the ICMPv6 code field filter <ul style="list-style-type: none"> <li>eq - Configures a specific ICMPv6 code. Specify the ICMPv6 code value.</li> <li>range - Configures a range of ICMPv6 code. Specify the starting and ending ICMPv6 code values.</li> </ul> <p><b>Note:</b> ICMPv6 packets with code field value matching the values specified here are dropped.</p>  |
| log                      | Logs all deny events matching this entry                                                                                                                                                                                                                                                                                                                                        |



|                          |                                                                                                                                                                                                                                                                                            |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| rule-precedence <1-5000> | <p>Assigns a precedence for this deny rule</p> <ul style="list-style-type: none"> <li>• &lt;1-5000&gt; – Specify a value from 1 - 5000.</li> </ul> <p><b>Note:</b> Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.</p> |
| rule-description <LINE>  | Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).                                                                                                               |

```
deny ipv6 [<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/MASK>|any|
host <DEST-HOST-IPv6>] (log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

|                          |                                                                                                                                                                                                                                                                                            |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ipv6                     | Applies this deny rule to IPv6 packets only                                                                                                                                                                                                                                                |
| <SOURCE-IPv6/MASK>       | Specifies a range of IPv6 source address (network) to match. IPv6 packets received from any source in the specified network are dropped.                                                                                                                                                   |
| any                      | Specifies the source as any IPv6 address. IPv6 packets received from any source are dropped.                                                                                                                                                                                               |
| host <SOURCE-HOST-IPv6>  | Identifies a specific host (as the source to match) by its IPv6 address. IPv6 packets received from the specified host are dropped. <ul style="list-style-type: none"> <li>• &lt;SOURCE-HOST-IPv6&gt; – Specify the source host's exact IPv6 address.</li> </ul>                           |
| <DEST-IPv6/MASK>         | Specifies a range of IPv6 destination address (network) to match. IPv6 packets addressed to any destination within the specified network are dropped.                                                                                                                                      |
| any                      | Specifies the destination as any IPv6 address. IPv6 packets addressed to any destination are dropped.                                                                                                                                                                                      |
| host <DEST-HOST-IPv6>    | Identifies a specific host (as the destination to match) by its IPv6 address. IPv6 packets addressed to the specified host are dropped. <ul style="list-style-type: none"> <li>• &lt;DEST-HOST-IPv6&gt; – Specify the destination host's exact IPv6 address.</li> </ul>                    |
| log                      | Logs all deny events matching this entry                                                                                                                                                                                                                                                   |
| rule-precedence <1-5000> | <p>Assigns a precedence for this deny rule</p> <ul style="list-style-type: none"> <li>• &lt;1-5000&gt; – Specify a value from 1 - 5000.</li> </ul> <p><b>Note:</b> Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.</p> |
| rule-description <LINE>  | Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).                                                                                                               |

```
deny proto [<PROTOCOL-NUMBER>|<PROTOCOL-NAME>|eigrp|gre|igmp|ospf|vrrp]
[<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/MASK>|any|host <DEST-HOST-
IPv6>]
(log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

|                   |                                                                                                                                                               |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| proto             | Configures the ACL for additional protocols<br>Additional protocols (other than IP, ICMP, TCP, and UDP) must be configured using this parameter.              |
| <PROTOCOL-NUMBER> | Filters protocols using their IANA protocol number <ul style="list-style-type: none"> <li>• &lt;PROTOCOL-NUMBER&gt; – Specify the protocol number.</li> </ul> |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <PROTOCOL-NAME>         | Filters protocols using their IANA protocol name <ul style="list-style-type: none"> <li>&lt;PROTOCOL-NAME&gt; – Specify the protocol name.</li> </ul>                                                                                                                                                                                                                                                                                                                                              |
| eigrp                   | Identifies the EIGRP protocol (number 88)<br>EIGRP enables routers to maintain copies of neighbors' routing tables. Routers use this information to determine the fastest route to a destination. When a router fails to find a route in its stored route tables, it sends a query to neighbors who in turn query their neighbors till a route is found. EIGRP also enables routers to inform neighbors of changes in their routing tables.                                                        |
| gre                     | Identifies the GRE protocol (number 47)<br>GRE is a tunneling protocol that enables transportation of protocols (IP, IPX, DEC net, etc.) over an IP network. GRE encapsulates the packet at the source and removes the encapsulation at the destination.                                                                                                                                                                                                                                           |
| igp                     | Identifies any private internal gateway (primarily used by CISCO for their IGRP) (number 9)<br>IGP enables exchange of information between hosts and routers within a managed network. The most commonly used IGP protocols are: RIP and OSPF.                                                                                                                                                                                                                                                     |
| ospf                    | Identifies the OSPF protocol (number 89)<br>OSPF is a link-state IGP. OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets.                                                      |
| vrrp                    | Identifies the VRRP protocol (number 112)<br>VRRP allows a pool of routers to be advertised as a single virtual router. This virtual router is configured by hosts as their default gateway. VRRP elects a master router, from this pool, and assigns it a virtual IP address. The master router routes and forwards packets to hosts on the same subnet. When the master router fails, one of the backup routers is elected as the master and its IP address is mapped to the virtual IP address. |
| <SOURCE-IPv6/MASK>      | Specifies a range of IPv6 source address (network) to match. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from any source in the specified network are dropped.                                                                                                                                                                                                                                                                                                                         |
| any                     | Specifies the source as any IPv6 address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from any source are dropped.                                                                                                                                                                                                                                                                                                                                                                     |
| host <SOURCE-HOST-IPv6> | Identifies a specific host (as the source to match) by its IPv6 address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the specified host are dropped. <ul style="list-style-type: none"> <li>&lt;SOURCE-HOST-IP&gt; – Specify the source host's exact IPv6 address.</li> </ul>                                                                                                                                                                                                     |
| <DEST-IPv6/MASK>        | Specifies a range of IPv6 destination address (network) to match. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to any destination within the specified network are dropped.                                                                                                                                                                                                                                                                                                            |
| any                     | Specifies the destination as any IPv6 address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to any destination are dropped.                                                                                                                                                                                                                                                                                                                                                            |
| host <DEST-HOST-IPv6>   | Identifies a specific host (as the destination to match) by its IPv6 address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to the specified host are dropped. <ul style="list-style-type: none"> <li>&lt;DEST-HOST-IPv6&gt; – Specify the destination host's exact IPv6 address.</li> </ul>                                                                                                                                                                                            |

|                          |                                                                                                                                                                                                                                                                                            |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| log                      | Logs all deny events matching this entry                                                                                                                                                                                                                                                   |
| rule-precedence <1-5000> | <p>Assigns a precedence for this deny rule</p> <ul style="list-style-type: none"> <li>• &lt;1-5000&gt; – Specify a value from 1 - 5000.</li> </ul> <p><b>Note:</b> Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.</p> |
| rule-description <LINE>  | Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).                                                                                                               |

```
deny [tcp|udp] [<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/MASK>|any|
eq <SOURCE-PORT>|host <DEST-HOST-IPv6>|range <START-PORT> <END-PORT>] [eq [<1-65535>|
<SERVICE-NAME>|
bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|ntp|pop3|sip|smtp|ssh|telnet|tftp|www]|
range <START-PORT> <END-PORT>] (log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

|                               |                                                                                                                                                                                                                                                                        |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| tcp                           | Applies this deny rule to TCP packets only                                                                                                                                                                                                                             |
| udp                           | Applies this deny rule to UDP packets only                                                                                                                                                                                                                             |
| <SOURCE-IPv6/MASK>            | This keyword is common to the 'tcp' and 'udp' parameters. Specifies a range of IPv6 source address (network) to match. TCP/UDP packets received from any source in the specified network are dropped.                                                                  |
| any                           | This keyword is common to the 'tcp' and 'udp' parameters. Specifies the source as any IPv6 address. TCP/UDP packets received from any source are dropped.                                                                                                              |
| host <SOURCE-HOST-IPv6>       | Identifies a specific host (as the source to match) by its IPv6 address. TCP/UDP packets received from the specified host are dropped. <ul style="list-style-type: none"> <li>• &lt;SOURCE-HOST-IP&gt; – Specify the source host's exact IPv6 address.</li> </ul>      |
| <DEST-IPv6/MASK>              | This keyword is common to the 'tcp' and 'udp' parameters. Specifies a range of IPv6 destination address (network) to match. TCP/UDP packets addressed to any destination within the specified network are dropped.                                                     |
| any                           | This keyword is common to the 'tcp' and 'udp' parameters. Specifies the destination as any destination IPv6 address. TCP/UDP packets received from any destination are dropped.                                                                                        |
| eq <SOURCE-PORT>              | Identifies a specific source port <ul style="list-style-type: none"> <li>• &lt;SOURCE-PORT&gt; – Specify the exact source port.</li> </ul>                                                                                                                             |
| host <DEST-HOST-IP>           | Identifies a specific host (as the destination to match) by its IPv6 address. TCP/UDP packets addressed to the specified host are dropped. <ul style="list-style-type: none"> <li>• &lt;DEST-HOST-IP&gt; – Specify the destination host's exact IP address.</li> </ul> |
| range <START-PORT> <END-PORT> | Specifies a range of source ports <ul style="list-style-type: none"> <li>• &lt;START-PORT&gt; – Specify the first port in the range.</li> <li>• &lt;END-PORT&gt; – Specify the last port in the range.</li> </ul>                                                      |

|                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| eq [<1-65535>  <SERVICE-NAME> <br> bgp dns ftp  ftp-data gropher <br>https ldap nntp ntp  pop3 sip <br>smtp  ssh telnet  tftp www] | Identifies a specific destination or protocol port to match <ul style="list-style-type: none"> <li>• &lt;1-65535&gt; – The destination port is designated by its number</li> <li>• &lt;SERVICE-NAME&gt; – Specifies the service name</li> <li>• bgp – The designated BGP protocol port (179)</li> <li>• dns – The designated DNS protocol port (53)</li> <li>• ftp – The designated FTP protocol port (21)</li> <li>• ftp-data – The designated FTP data port (20)</li> <li>• gropher – The designated GROPER protocol port (70)</li> <li>• https – The designated HTTPS protocol port (443)</li> <li>• ldap – The designated LDAP protocol port (389)</li> <li>• nntp – The designated NNTP protocol port (119)</li> <li>• ntp – The designated NTP protocol port (123)</li> <li>• pop3 – The designated POP3 protocol port (110)</li> <li>• sip – The designated SIP protocol port (5060)</li> <li>• smtp – The designated SMTP protocol port (25)</li> <li>• ssh – The designated SSH protocol port (22)</li> <li>• telnet – The designated Telnet protocol port (23)</li> <li>• tftp – The designated TFTP protocol port (69)</li> <li>• www – The designated www protocol port (80)</li> </ul> |
| range <START-PORT> <END-PORT>                                                                                                      | Specifies a range of destination ports <ul style="list-style-type: none"> <li>• &lt;START-PORT&gt; – Specify the first port in the range. <ul style="list-style-type: none"> <li>• &lt;END-PORT&gt; – Specify the last port in the range.</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| log                                                                                                                                | Logs all deny events matching this entry                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| rule-precedence <1-5000>                                                                                                           | Assigns a precedence for this deny rule <ul style="list-style-type: none"> <li>• &lt;1-5000&gt; – Specify a value from 1 - 5000.</li> </ul> <p><b>Note:</b> Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| rule-description <LINE>                                                                                                            | Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## Examples

```

nx9500-6C8809(config-ipv6-acl-test)#deny icmpv6 any any type eq 1 code eq 0 log rule-
precedence 1
nx9500-6C8809(config-ipv6-acl-test)#show context
ipv6 access-list test
 deny icmpv6 any any type eq destination-unreachable code eq router-renumbering-command
 log rule-precedence 1
nx9500-6C8809(config-ipv6-acl-test)#

```

## Related Commands

|                                            |                                                         |
|--------------------------------------------|---------------------------------------------------------|
| <a href="#">no (ipv6-acl)</a> on page 1414 | Removes a specified deny access rule from this IPv6 ACL |
|--------------------------------------------|---------------------------------------------------------|

## permit (ipv6-acl)

Creates a permit rule that accepts packets from a specified IPv6 source and/or addressed to a specified IPv6 destination. You can also use this command to modify an existing permit rule.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
permit [icmpv6|ipv6|proto|tcp|udp]
permit icmpv6 [<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/MASK>|any|
host <DEST-HOST-IPv6>] [code [eq <ICMPv6-CODE>|range <STARTING-ICMPv6-CODE> <ENDING-ICMPv6-
CODE>]]
type [eq <ICMPv6-TYPE>|range <STARTING-ICMPv6-TYPE> <ENDING-ICMPv6-TYPE>]]
(log,rule-precedence <1-5000>) {(rule-description <LINE>)}
permit ipv6 [<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/MASK>|any|
host <DEST-HOST-IPv6>] (log,rule-precedence <1-5000>) {(rule-description <LINE>)}
permit proto [<PROTOCOL-NUMBER>|<PROTOCOL-NAME>|eigrp|gre|igmp|ospf|vrrp]
[<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/MASK>|any|host <DEST-HOST-
IPv6>]
(log,rule-precedence <1-5000>) {(rule-description <LINE>)}
permit [tcp|udp] [<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/MASK>|any|
eq <SOURCE-PORT>|host <DEST-HOST-IPv6>|range <START-PORT> <END-PORT>] [eq [<1-65535>|<
SERVICE-NAME>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|ntp|pop3|sip|smtp|ssh|telnet|
tftp|www]]
range <START-PORT> <END-PORT>] (log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

### Parameters

```
permit icmpv6 [<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/MASK>|any|
host <DEST-HOST-IPv6>] [code [eq <ICMPv6-CODE>|range <STARTING-ICMPv6-CODE> <ENDING-ICMPv6-
CODE>]]
type [eq <ICMPv6-TYPE>|range <STARTING-ICMPv6-TYPE> <ENDING-ICMPv6-TYPE>]]
(log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

|                         |                                                                                                                                                                                                                                                                    |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| icmpv6                  | Applies this permit rule to ICMPv6 packets only                                                                                                                                                                                                                    |
| <SOURCE-IPv6/MASK>      | Specifies a range of IPv6 source address (network) to match. ICMPv6 packets received from any source in the specified network are forwarded.                                                                                                                       |
| any                     | Specifies the source as any IPv6 address. ICMPv6 packets received from any source are forwarded.                                                                                                                                                                   |
| host <SOURCE-HOST-IPv6> | Identifies a specific host (as the source to match) by its IPv6 address. ICMPv6 packets received from the specified host are forwarded. <ul style="list-style-type: none"><li>• &lt;SOURCE-HOST-IPv6&gt; - Specify the source host's exact IPv6 address.</li></ul> |
| <DEST-IPv6/MASK>        | Specifies a range of IPv6 destination address (network) to match. ICMPv6 packets addressed to any destination within the specified network are forwarded.                                                                                                          |
| any                     | Specifies the destination as any IPv6 address. ICMPv6 packets addressed to any destination are forwarded.                                                                                                                                                          |

|                          |                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| host <DEST-HOST-IPv6>    | Identifies a specific host (as the destination to match) by its IPv6 address. ICMPv6 packets addressed to the specified host are forwarded. <ul style="list-style-type: none"> <li>&lt;DEST-HOST-IPv6&gt; – Specify the destination host’s exact IPv6 address.</li> </ul>                                                                                                         |
| <ICMPv6-TYPE> [eq range] | Defines the ICMPv6 type field filter <ul style="list-style-type: none"> <li>eq – Configures a specific ICMPv6 type. Specify the ICMPv6 type value.</li> <li>range – Configures a range of ICMPv6 types. Specify the starting and ending ICMPv6 type values.</li> </ul> <p><b>Note:</b> ICMPv6 packets with type field value matching the values specified here are forwarded.</p> |
| <ICMPv6-CODE>            | Defines the ICMPv6 code field filter <ul style="list-style-type: none"> <li>eq – Configures a specific ICMPv6 code. Specify the ICMPv6 code value.</li> <li>range – Configures a range of ICMPv6 code. Specify the starting and ending ICMPv6 code values.</li> </ul> <p><b>Note:</b> ICMPv6 packets with code field value matching the values specified here are forwarded.</p>  |
| log                      | Logs all permit events matching this entry                                                                                                                                                                                                                                                                                                                                        |
| rule-precedence <1-5000> | Assigns a precedence for this permit rule <ul style="list-style-type: none"> <li>&lt;1-5000&gt; – Specify a value from 1 - 5000.</li> </ul> <p><b>Note:</b> Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.</p>                                                                                               |
| rule-description <LINE>  | Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).                                                                                                                                                                                                    |

```
permit ipv6 [<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/MASK>|any|
host <DEST-HOST-IPv6>] (log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

|                         |                                                                                                                                                                                                                                                                         |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ipv6                    | Applies this permit rule to IPv6 packets only                                                                                                                                                                                                                           |
| <SOURCE-IPv6/MASK>      | Specifies a range of IPv6 source address (network) to match. IPv6 packets received from any source in the specified network are forwarded.                                                                                                                              |
| any                     | Specifies the source as any IPv6 address. IPv6 packets received from any source are forwarded.                                                                                                                                                                          |
| host <SOURCE-HOST-IPv6> | Identifies a specific host (as the source to match) by its IPv6 address. IPv6 packets received from the specified host are forwarded. <ul style="list-style-type: none"> <li>&lt;SOURCE-HOST-IPv6&gt; – Specify the source host’s exact IPv6 address.</li> </ul>        |
| <DEST-IPv6/MASK>        | Specifies a range of IPv6 destination address (network) to match. IPv6 packets addressed to any destination within the specified network are forwarded.                                                                                                                 |
| any                     | Specifies the destination as any IPv6 address. IPv6 packets addressed to any destination are forwarded.                                                                                                                                                                 |
| host <DEST-HOST-IPv6>   | Identifies a specific host (as the destination to match) by its IPv6 address. IPv6 packets addressed to the specified host are forwarded. <ul style="list-style-type: none"> <li>&lt;DEST-HOST-IPv6&gt; – Specify the destination host’s exact IPv6 address.</li> </ul> |

|                          |                                                                                                                                                                                                                                                                                              |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| log                      | Logs all permit events matching this entry                                                                                                                                                                                                                                                   |
| rule-precedence <1-5000> | <p>Assigns a precedence for this permit rule</p> <ul style="list-style-type: none"> <li>• &lt;1-5000&gt; - Specify a value from 1 - 5000.</li> </ul> <p><b>Note:</b> Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.</p> |
| rule-description <LINE>  | Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).                                                                                                               |

```

permit proto [<PROTOCOL-NUMBER>|<PROTOCOL-NAME>|eigrp|gre|igp|ospf|vrrp]
[<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/MASK>|any|host <DEST-HOST-IPv6>]
(log,rule-precedence <1-5000>) {(rule-description <LINE>)}

```

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| proto             | Configures the ACL for additional protocols<br>Additional protocols (other than IP, ICMP, TCP, and UDP) must be configured using this parameter.                                                                                                                                                                                                                                                                                                                                                   |
| <PROTOCOL-NUMBER> | Filters protocols using their IANA protocol number <ul style="list-style-type: none"> <li>• &lt;PROTOCOL-NUMBER&gt; - Specify the protocol number.</li> </ul>                                                                                                                                                                                                                                                                                                                                      |
| <PROTOCOL-NAME>   | Filters protocols using their IANA protocol name <ul style="list-style-type: none"> <li>• &lt;PROTOCOL-NAME&gt; - Specify the protocol name.</li> </ul>                                                                                                                                                                                                                                                                                                                                            |
| eigrp             | Identifies the EIGRP protocol (number 88)<br>EIGRP enables routers to maintain copies of neighbors' routing tables. Routers use this information to determine the fastest route to a destination. When a router fails to find a route in its stored route tables, it sends a query to neighbors who in turn query their neighbors till a route is found. EIGRP also enables routers to inform neighbors of changes in their routing tables.                                                        |
| gre               | Identifies the GRE protocol (number 47)<br>GRE is a tunneling protocol that enables transportation of protocols (IP, IPX, DEC net, etc.) over an IP network. GRE encapsulates the packet at the source and removes the encapsulation at the destination.                                                                                                                                                                                                                                           |
| igp               | Identifies any private internal gateway (primarily used by CISCO for their IGRP) (number 9)<br>IGP enables exchange of information between hosts and routers within a managed network. The most commonly used IGP protocols are: RIP and OSPF.                                                                                                                                                                                                                                                     |
| ospf              | Identifies the OSPF protocol (number 89)<br>OSPF is a link-state IGP. OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets.                                                      |
| vrrp              | Identifies the VRRP protocol (number 112)<br>VRRP allows a pool of routers to be advertised as a single virtual router. This virtual router is configured by hosts as their default gateway. VRRP elects a master router, from this pool, and assigns it a virtual IP address. The master router routes and forwards packets to hosts on the same subnet. When the master router fails, one of the backup routers is elected as the master and its IP address is mapped to the virtual IP address. |

|                          |                                                                                                                                                                                                                                                                                                           |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <SOURCE-IPv6/MASK>       | Specifies a range of IPv6 source address (network) to match. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from any source in the specified network are forwarded.                                                                                                                              |
| any                      | Specifies the source as any IPv6 address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from any source are forwarded.                                                                                                                                                                          |
| host <SOURCE-HOST-IPv6>  | Identifies a specific host (as the source to match) by its IPv6 address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the specified host are forwarded. <ul style="list-style-type: none"> <li>&lt;SOURCE-HOST-IP&gt; - Specify the source host's exact IPv6 address.</li> </ul>          |
| <DEST-IPv6/MASK>         | Specifies a range of IPv6 destination address (network) to match. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to any destination within the specified network are forwarded.                                                                                                                 |
| any                      | Specifies the destination as any IPv6 address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to any destination are forwarded.                                                                                                                                                                 |
| host <DEST-HOST-IPv6>    | Identifies a specific host (as the destination to match) by its IPv6 address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to the specified host are forwarded. <ul style="list-style-type: none"> <li>&lt;DEST-HOST-IPv6&gt; - Specify the destination host's exact IPv6 address.</li> </ul> |
| log                      | Logs all permit events matching this entry                                                                                                                                                                                                                                                                |
| rule-precedence <1-5000> | Assigns a precedence for this permit rule <ul style="list-style-type: none"> <li>&lt;1-5000&gt; - Specify a value from 1 - 5000.</li> </ul> <p><b>Note:</b> Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.</p>                       |
| rule-description <LINE>  | Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).                                                                                                                            |

```

permit [tcp|udp] [<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/MASK>|any|
eq <SOURCE-PORT>|host <DEST-HOST-IPv6>|range <START-PORT> <END-PORT>] [eq [<1-65535>|
<SERVICE-NAME>|
bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|ntp|pop3|sip|smtp|ssh|telnet|tftp|www|
range <START-PORT> <END-PORT>] (log,rule-precedence <1-5000>) {(rule-description <LINE>)}

```

|                         |                                                                                                                                                                                                                                                                   |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| tcp                     | Applies this permit rule to TCP packets only                                                                                                                                                                                                                      |
| udp                     | Applies this permit rule to UDP packets only                                                                                                                                                                                                                      |
| <SOURCE-IPv6/MASK>      | This keyword is common to the 'tcp' and 'udp' parameters. Specifies a range of IPv6 source address (network) to match. TCP/UDP packets received from any source in the specified network are forwarded.                                                           |
| any                     | This keyword is common to the 'tcp' and 'udp' parameters. Specifies the source as any IPv6 address. TCP/UDP packets received from any source are forwarded.                                                                                                       |
| host <SOURCE-HOST-IPv6> | Identifies a specific host (as the source to match) by its IPv6 address. TCP/UDP packets received from the specified host are forwarded. <ul style="list-style-type: none"> <li>&lt;SOURCE-HOST-IP&gt; - Specify the source host's exact IPv6 address.</li> </ul> |



|                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <DEST-IPv6/MASK>                                                                                                                   | This keyword is common to the 'tcp' and 'udp' parameters. Specifies a range of IPv6 destination address (network) to match. TCP/UDP packets addressed to any destination within the specified network are forwarded.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| any                                                                                                                                | This keyword is common to the 'tcp' and 'udp' parameters. Specifies the destination as any destination IPv6 address. TCP/UDP packets received from any destination are forwarded.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| eq <SOURCE-PORT>                                                                                                                   | Identifies a specific source port <ul style="list-style-type: none"> <li>&lt;SOURCE-PORT&gt; - Specify the exact source port.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| host <DEST-HOST-IP>                                                                                                                | Identifies a specific host (as the destination to match) by its IPv6 address. TCP/UDP packets addressed to the specified host are forwarded. <ul style="list-style-type: none"> <li>&lt;DEST-HOST-IP&gt; - Specify the destination host's exact IP address.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| range <START-PORT> <END-PORT>                                                                                                      | Specifies a range of source ports <ul style="list-style-type: none"> <li>&lt;START-PORT&gt; - Specify the first port in the range.</li> <li>&lt;END-PORT&gt; - Specify the last port in the range.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| eq [<1-65535>  <SERVICE-NAME> <br> bgp dns ftp  ftp-data gropher <br>https ldap nntp ntp  pop3 sip <br>smtp  ssh telnet  tftp www] | Identifies a specific destination or protocol port to match <ul style="list-style-type: none"> <li>&lt;1-65535&gt; - The destination port is designated by its number</li> <li>&lt;SERVICE-NAME&gt; - Specifies the service name</li> <li>bgp - The designated BGP protocol port (179)</li> <li>dns - The designated DNS protocol port (53)</li> <li>ftp - The designated FTP protocol port (21)</li> <li>ftp-data - The designated FTP data port (20)</li> <li>gropher - The designated GROPPER protocol port (70)</li> <li>https - The designated HTTPS protocol port (443)</li> <li>ldap - The designated LDAP protocol port (389)</li> <li>nntp - The designated NNTP protocol port (119)</li> <li>ntp - The designated NTP protocol port (123)</li> <li>pop3 - The designated POP3 protocol port (110)</li> <li>sip - The designated SIP protocol port (5060)</li> <li>smtp - The designated SMTP protocol port (25)</li> <li>ssh - The designated SSH protocol port (22)</li> <li>telnet - The designated Telnet protocol port (23)</li> <li>tftp - The designated TFTP protocol port (69)</li> <li>www - The designated www protocol port (80)</li> </ul> |
| range <START-PORT> <END-PORT>                                                                                                      | Specifies a range of destination ports <ul style="list-style-type: none"> <li>&lt;START-PORT&gt; - Specify the first port in the range.</li> <li>&lt;END-PORT&gt; - Specify the last port in the range.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| log                                                                                                                                | Logs all permit events matching this entry                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

|                          |                                                                                                                                                                                                                                                                                            |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| rule-precedence <1-5000> | <p>Assigns a precedence for this permit rule</p> <ul style="list-style-type: none"> <li>&lt;1-5000&gt; – Specify a value from 1 - 5000.</li> </ul> <p><b>Note:</b> Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.</p> |
| rule-description <LINE>  | Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).                                                                                                             |

### Examples

```

nx9500-6C8809(config-ipv6-acl-test)#permit proto gre any any log rule-precedence 2
nx9500-6C8809(config-ipv6-acl-test)#show context
ipv6 access-list test
 deny icmpv6 any any type eq destination-unreachable code eq router-renumbering-command
 log rule-precedence 1
 permit proto gre any any log rule-precedence 2
nx9500-6C8809(config-ipv6-acl-test)#

```

### Related Commands

|                                            |                                                           |
|--------------------------------------------|-----------------------------------------------------------|
| <a href="#">no (ipv6-acl)</a> on page 1414 | Removes a specified permit access rule from this IPv6 ACL |
|--------------------------------------------|-----------------------------------------------------------|

### *no (ipv6-acl)*

Removes a deny or permit rule from this IPv6 ACL Policy

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```

no [deny|permit]
no [deny|permit] [icmpv6|ipv6|proto|tcp|udp] <RULE-PARAMETERS> {(rule-description <LINE>)}

```

#### Parameters

no <PARAMETERS>

|                 |                                                                  |
|-----------------|------------------------------------------------------------------|
| no <PARAMETERS> | Removes a deny or permit rule from the selected IPv6 access list |
|-----------------|------------------------------------------------------------------|

### Examples

The following example shows the ACL 'test' settings before the 'no' commands is executed:

```

nx9500-6C8809(config-ipv6-acl-test)#show context
ipv6 access-list test
 deny icmpv6 any any type eq destination-unreachable code eq router-renumbering-command
 log rule-precedence 1

```

```

permit proto gre any any log rule-precedence 2
nx9500-6C8809(config-ipv6-acl-test)#
nx9500-6C8809(config-ipv6-acl-test)#no deny icmpv6 any any type eq 1 log rule-precedence 1
nx9500-6C8809(config-ipv6-acl-test)#show context
ipv6 access-list test
 permit proto gre any any log rule-precedence 2
nx9500-6C8809(config-ipv6-acl-test)#

```

## ip-snmp-access-list

SNMP performs network management functions using a data structure called a MIB (Management Information Base). SNMP is widely implemented but not very secure, since it uses only text community strings for accessing controller or service platform configuration files.

Use SNMP ACLs to help reduce SNMP vulnerabilities, as SNMP traffic can be exploited to produce a DoS (denial of service).

The following table summarizes SNMP access list configuration commands:

**Table 38: SNMP Access List Config Mode Commands**

| Command                                           | Description                                           |
|---------------------------------------------------|-------------------------------------------------------|
| <a href="#">deny (ip-snmp acl)</a> on page 1415   | Creates a deny SNMP MIB object traffic rule           |
| <a href="#">permit (ip-snmp acl)</a> on page 1416 | Creates a permit SNMP MIB object traffic rule         |
| <a href="#">no (ip-snmp acl)</a> on page 1417     | Removes a deny or permit SNMP MIB object traffic rule |

### *deny (ip-snmp acl)*

Creates a deny SNMP MIB object traffic rule. Use this command to specify the match criteria based on which SNMP traffic is denied

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
deny [<IP/M>|any|host <IP>]
```

#### Parameters

```
deny [<IP/M>|any|host <IP>]
```

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| deny [<IP/M> any host <IP>] | <p>Configures the match criteria for this deny rule</p> <ul style="list-style-type: none"> <li>• &lt;IP/M&gt; - Specifies a network address and mask in the A.B.C.D/M format. Packets received from or destined for this network are dropped.</li> <li>• any - Specifies the match criteria as any. Packets received from or destined for any address are dropped.</li> <li>• host &lt;IP&gt; - Identifies a host by its IP address. Packets received from or destined for this host are dropped.</li> </ul> |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-ip-snmp-acl-test)#deny 192.168.13.0/24
nx9500-6C8809(config-ip-snmp-acl-test)#show context
ip snmp-access-list test
 deny 192.168.13.0/24
nx9500-6C8809(config-ip-snmp-acl-test)#
```

## Related Commands

|                                               |                                             |
|-----------------------------------------------|---------------------------------------------|
| <code>no (ip-snmp acl) on</code><br>page 1417 | Removes this deny rule form the IP SNMP ACL |
|-----------------------------------------------|---------------------------------------------|

### *permit (ip-snmp acl)*

Creates a permit SNMP MIB object traffic rule. Use this command to specify the match criteria based on which SNMP traffic is permitted.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
permit [<IP/M>|any|host <IP>]
```

## Parameters

```
permit [<IP/M>|any|host <IP>]
```

|                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>permit [&lt;IP/M&gt; any host &lt;IP&gt;]</code> | Configures the match criteria for this permit rule <ul style="list-style-type: none"><li>• &lt;IP/M&gt; - Specifies a network address and mask in the A.B.C.D/M format. Packets received from or destined for this network are forwarded.</li><li>• any - Specifies the match criteria as any. Packets received from or destined for any address are forwarded.</li><li>• host &lt;IP&gt; - Identifies a host by its IP address. Packets received from or destined for this host are forwarded.</li></ul> |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-ip-snmp-acl-test)#permit host 192.168.13.13
nx9500-6C8809(config-ip-snmp-acl-test)#show context
ip snmp-access-list test
 permit host 192.168.13.13
 deny 192.168.13.0/24
nx9500-6C8809(config-ip-snmp-acl-test)#
```

## Related Commands

|                                               |                                               |
|-----------------------------------------------|-----------------------------------------------|
| <code>no (ip-snmp acl) on</code><br>page 1417 | Removes this permit rule form the IP SNMP ACL |
|-----------------------------------------------|-----------------------------------------------|

*no (ip-snmp acl)*

Removes a deny or permit rule from the IP SNMP ACL. Use this command to remove IP SNMP ACL as they become obsolete for filtering network access permissions.

**Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

**Syntax**

```
no [deny|permit] [<IP/M>|any|host <IP>]
```

**Parameters**

```
no <PARAMETERS>
```

|                 |                                                              |
|-----------------|--------------------------------------------------------------|
| no <PARAMETERS> | Removes deny and/or permit access rule from this IP SNMP ACL |
|-----------------|--------------------------------------------------------------|

**Usage Guidelines**

- 

**Examples**

```
nx9500-6C8809(config-ip-snmp-acl-test)#show context
ip snmp-access-list test
 permit host 192.168.13.13
 deny 192.168.13.0/24
nx9500-6C8809(config-ip-snmp-acl-test)#
nx9500-6C8809(config-ip-snmp-acl-test)#no permit host 192.168.13.13
nx9500-6C8809(config-ip-snmp-acl-test)#show context
ip snmp-access-list test
 deny 192.168.13.0/24
nx9500-6C8809(config-ip-snmp-acl-test)#
```

## ex3500-ext-access-list

An IPv4 EX3500 extended ACL is a policy-based ACL that either prevents or allows specific clients from using the EX35XX (EX3524 or EX3548) switch. It allows you to permit or deny client access by specifying that the traffic from a specific host or network and/or the traffic to a specific host or network be either denied or permitted.

An EX3500 extended ACL consists of a set of deny /permit rules that filter packets based on both source and destination IPv4 addresses. Each rule specifies a set of match criteria (the source and destination IP addresses) and has a unique precedence value assigned. These ACL rules are applied sequentially to the traffic at a port, by a firewall-supported device, in an increasing order of their precedence. When a packet matches the criteria specified in a rule the packet is either forwarded or dropped based on the rule type.

The following table summarizes IPv4 EX3500 extended ACL configuration commands:

**Table 39: EX3500 Extended Access List Config Mode Commands**

| Command                                              | Description                                                                                                                                                          |
|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">deny (ex3500-ext acl)</a> on page 1418   | Creates a deny access rule or modifies an existing rule. A deny access rule rejects packets from specified address(es) and/or destined to specified address(es).     |
| <a href="#">permit (ex3500-ext acl)</a> on page 1420 | Creates a permit access rule or modifies an existing rule. A permit access rule accepts packets from specified address(es) and/or destined to specified address(es). |
| <a href="#">no (ex3500-ext acl)</a> on page 1423     | Removes a deny and/or a permit access rule from this IPv4 EX3500 extended ACL                                                                                        |

**Note**

To implement the EX3500 extended ACL, apply it directly to a EX35XX device, or to an EX35XX profile. For more information, see [access-group](#) on page 1299.

*deny (ex3500-ext acl)*

Creates a deny ACL rule that filters packets based on the source and/or destination IPv4 address, and other specified criteria. You can also use this command to modify an existing deny rule.

**Supported in the following platforms:**

- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

**Syntax**

```
deny [<0-255>|tcp|udp] [<SOURCE-NETWORK-IP/MASK>|any|host <SOURCE-HOST-IP>]
[<DEST-NETWORK-IP/MASK>|any|host <DEST-HOST-IP>] [control-flag <0-63>|
destination-port <0-65535>|destination-port-bitmark <0-65535>|dscp <0-63>|
ex3500-time-range <TIME-RANGE-NAME>|ip-precedence <0-63>|rule-precedence <1-128>|
source-port <0-65535>|source-port-bitmark <0-65535>]
```

**Parameters**

```
deny [<0-255>|tcp|udp] [<SOURCE-NETWORK-IP/MASK>|any|host <SOURCE-HOST-IP>]
[<DEST-NETWORK-IP/MASK>|any|host <DEST-HOST-IP>] [control-flag <0-63>|
destination-port <0-65535>|destination-port-bitmark <0-65535>|dscp <0-63>|
ex3500-time-range <TIME-RANGE-NAME>|ip-precedence <0-63>|rule-precedence <1-128>|
source-port <0-65535>|source-port-bitmark <0-65535>]
```

|                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| deny [<0-255> tcp udp]                               | Creates a deny rule and identifies the protocol type. This deny rule is applied only to packets matching the protocol specified here.                                                                                                                                                                                                                                                                                  |
| [<SOURCE-NETWORK-IP/MASK> any host <SOURCE-HOST-IP>] | Specifies the source as any, host, or network <ul style="list-style-type: none"> <li>• &lt;SOURCE-NETWORK-IP/MASK&gt; - Configures a network as the source. Provide the network's IPv4 address along with the mask.</li> <li>• host &lt;SOURCE-HOST-IP&gt; - Configures a single device as the source. Provide the host device's IPv4 address.</li> <li>• any - Specifies that the source can be any device</li> </ul> |

|                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [<DEST-NETWORK-IP/MASK> <br>any] host <DEST-HOST-IP>] | <p>Specifies the destination as any, host, or network</p> <ul style="list-style-type: none"> <li>• &lt;DEST-NETWORK-IP/MASK&gt; – Configures a network as the destination. Provide the network’s IPv4 address along with the mask.</li> <li>• host &lt;DEST-HOST-IP&gt; – Configures a single device as the destination. Provide the host device’s IPv4 address.</li> <li>• any – Specifies that the destination can be any device</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| control-flag <0-63>                                   | <p>Configures the decimal number (representing a bit string) that specifies the control flag bits in byte 14 of the TCP header</p> <ul style="list-style-type: none"> <li>• &lt;0-63&gt; – Specify a value from 0 - 63.</li> </ul> <p><b>Note:</b> Control flags can be used only in ACLs designed to filter TCP traffic.</p> <p>The TCP header contains several one-bit boolean fields known as flags that influence flow of data across a TCP connection. Ignoring the CWR and ECE flags added for congestion notification by RFC 3168, there are six TCP control flags.</p> <ul style="list-style-type: none"> <li>• URG flag - Marks incoming packet as urgent.</li> <li>• ACK flag - Acknowledges receipt of packet</li> <li>• PUSH flag - Ensures that the packet is given appropriate priority. Often used at the beginning and end of data transfer.</li> <li>• RST flag - Resets the connection. Happens when remote host receives a establish connection packet, but does not have a service waiting to answer and sends a reply with reset flag.</li> <li>• SYN flag - Establishes the 3-way handshake between two hosts</li> <li>• FIN flag - Tears down the connection established between two hosts via the 3-way SYN process</li> </ul> |
| destination-port <0-65535>                            | <p>Configures the protocol destination port to match. The destination protocol can be TCP, UDP or any other protocol identified by its number (&lt;0-255&gt;).</p> <ul style="list-style-type: none"> <li>• &lt;0-65535&gt; – Specify the destination port from 0 - 65535.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| destination-port-bitmark<br><0-65535>                 | <p>Configures the decimal number representing the protocol destination port bits to match</p> <ul style="list-style-type: none"> <li>• &lt;0-65535&gt; – Specify the destination port bits from 0 - 65535.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| dscp <0-63>                                           | <p>Configures the DSCP priority level</p> <ul style="list-style-type: none"> <li>• &lt;0-63&gt; – Specify a value from 0 - 63.</li> </ul> <p><b>Note:</b> If specifying DSCP priority, ip-precedence cannot be specified.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| ex3500-time-range <TIME-<br>RANGE-NAME>               | <p>Applies a periodic or absolute time range to this rule</p> <ul style="list-style-type: none"> <li>• &lt;TIME-RANGE-NAME&gt; – Specify the time range name (should be existing and configured). For information on configuring EX3500 time-range, see <a href="#">ex3500</a>.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| ip-precedence <0-7>                                   | <p>Configures the IP header precedence</p> <ul style="list-style-type: none"> <li>• &lt;0-7&gt; – Specify a value from 0 - 7.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| source-port <0-65535>                                 | <p>Configures the protocol source port to match. The source protocol can be TCP, UDP or any other protocol identified by its number (&lt;0-255&gt;).</p> <ul style="list-style-type: none"> <li>• &lt;0-65535&gt; – Specify the source port from 0 - 65535.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| source-port-bitmark <0-65535> | Configures the decimal number representing the protocol source port bits to match <ul style="list-style-type: none"> <li>&lt;0-65535&gt; - Specify the source port bits from 0 - 65535.</li> </ul>                                                                                                                                                                                                                                                                  |
| rule-precedence <1-128>       | The following keywords are recursive and common to all of the above parameters: <ul style="list-style-type: none"> <li>rule-precedence - Assigns a precedence to this deny rule <ul style="list-style-type: none"> <li>&lt;1-128&gt; - Specify a value from 1 - 5000.</li> </ul> </li> </ul> <p><b>Note:</b> Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 4 and is applied first to packets.</p> |

### Usage Guidelines

Use this command to deny traffic between networks/hosts based on the protocol type selected in the access list configuration. The following protocols are supported:

- TCP
- UDP
- <0-255> (any Internet protocol other than TCP, UDP, and ICMP)

Packet content is checked against the ACEs in the ACL, and are allowed or denied access based on the ACL configuration.

- Filtering TCP/UDP allows you to specify port numbers as filtering criteria

### Examples

The following example denies TCP outgoing packets from all sources p within the 192.168.14.0/24 network to a specific host 192.168.13.13:

```
nx9500-6C8809(config-ip-ex3500-ext-acl-test)#deny tcp 192.168.14.0/24 host 192.168.13.13
rule-precedence 1
nx9500-6C8809(config-ip-ex3500-ext-acl-test)#show context
ip ex3500-ext-access-list test
 deny tcp 192.168.14.0/24 host 192.168.13.13 rule-precedence 1
nx9500-6C8809(config-ip-ex3500-ext-acl-test)#
```

### Related Commands

|                                     |                                                                                   |
|-------------------------------------|-----------------------------------------------------------------------------------|
| <code>no (ex3500-ext acl) on</code> | Removes a specified deny access rule from this IPv4 EX3500 extended ACL page 1423 |
|-------------------------------------|-----------------------------------------------------------------------------------|

*permit (ex3500-ext acl)*

Creates a permit ACL rule that filters packets based on the source and/or destination IPv4 address, and other specified criteria. You can also use this command to modify an existing permit rule.

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000



## Syntax

```
permit [<0-255>|tcp|udp] [<SOURCE-NETWORK-IP/MASK>|any|host <SOURCE-HOST-IP>]
[<DEST-NEWORK-IP/MASK>|any|host <DEST-HOST-IP>] [control-flag <0-63>|destination-port
<0-65535>|
destination-port-bitmark <0-65535>|dscp <0-63>|ex3500-time-range <TIME-RANGE-NAME>|
ip-precedence <0-63>|rule-precedence <1-128>|source-port <0-65535>|source-port-bitmark
<0-65535>]
```

## Parameters

```
permit [<0-255>|tcp|udp] [<SOURCE-NETWORK-IP/MASK>|any|host <SOURCE-HOST-IP>]
[<DEST-NEWORK-IP/MASK>|any|host <DEST-HOST-IP>] [control-flag <0-63>|destination-port
<0-65535>|
destination-port-bitmark <0-65535>|dscp <0-63>|ex3500-time-range <TIME-RANGE-NAME>|
ip-precedence <0-63>|rule-precedence <1-128>|source-port <0-65535>|source-port-bitmark
<0-65535>]
```

|                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| permit [<0-255> tcp udp]                             | Creates a permit rule, and identifies the protocol type. This permit rule is applied only to packets matching the protocol specified here.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| [<SOURCE-NETWORK-IP/MASK> any host <SOURCE-HOST-IP>] | Specifies the source as any, host, or network <ul style="list-style-type: none"><li>&lt;SOURCE-NETWORK-IP/MASK&gt; - Configures a network as the source. Provide the network's IPv4 address along with the mask.</li><li>host &lt;SOURCE-HOST-IP&gt; - Configures a single device as the source. Provide the host device's IPv4 address.</li><li>any - Specifies that the source can be any device</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| [<DEST-NETWORK-IP/MASK> any host <DEST-HOST-IP>]     | Specifies the destination as any, host, or network <ul style="list-style-type: none"><li>&lt;DEST-NETWORK-IP/MASK&gt; - Configures a network as the destination. Provide the network's IPv4 address along with the mask.</li><li>host &lt;DEST-HOST-IP&gt; - Configures a single device as the destination. Provide the host device's IPv4 address.</li><li>any - Specifies that the destination can be any device</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| control-flag <0-63>                                  | Configures the decimal number (representing a bit string) that specifies the control flag bits in byte 14 of the TCP header <ul style="list-style-type: none"><li>&lt;0-63&gt; - Specify a value from 0 - 63.</li></ul> <p><b>Note:</b> Control flags can be used only in ACLs designed to filter TCP traffic.</p> <p>The TCP header contains several one-bit boolean fields known as flags that influence flow of data across a TCP connection. Ignoring the CWR and ECE flags added for congestion notification by RFC 3168, there are six TCP control flags.</p> <ul style="list-style-type: none"><li>URG flag - Marks incoming packet as urgent</li><li>ACK flag - Acknowledges receipt of packet</li><li>PUSH flag - Ensures that the packet is given appropriate priority. Often used at the beginning and end of data transfer.</li><li>RST flag - Resets the connection. Happens when remote host receives a establish connection packet, but does not have a service waiting to answer and sends a reply with reset flag.</li><li>SYN flag - Establishes the 3-way handshake between two hosts</li><li>FIN flag - Tears down the connection established between two hosts via the 3-way SYN process</li></ul> |

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| destination-port <0-65535>          | Configures the protocol destination port to match. The destination protocol can be TCP, UDP or any other protocol identified by its number (<0-255>). <ul style="list-style-type: none"> <li>&lt;0-65535&gt; - Specify the destination port from 0 - 65535.</li> </ul>                                                                                                                                                                                                |
| destination-port-bitmark <0-65535>  | Configures the decimal number representing the protocol destination port bits to match <ul style="list-style-type: none"> <li>&lt;0-65535&gt; - Specify the destination port bits from 0 - 65535.</li> </ul>                                                                                                                                                                                                                                                          |
| dscp <0-63>                         | Configures the DSCP priority level <ul style="list-style-type: none"> <li>&lt;0-63&gt; - Specify a value from 0 - 63.</li> </ul> <p><b>Note:</b> If specifying DSCP priority, ip-precedence cannot be specified.</p>                                                                                                                                                                                                                                                  |
| ex3500-time-range <TIME-RANGE-NAME> | Applies a periodic or absolute time range to this rule <ul style="list-style-type: none"> <li>&lt;TIME-RANGE-NAME&gt; - Specify the time range name (should be existing and configured). For information on configuring EX3500 time-range, see <a href="#">ex3500</a>.</li> </ul>                                                                                                                                                                                     |
| ip-precedence <0-7>                 | Configures the IP header precedence <ul style="list-style-type: none"> <li>&lt;0-7&gt; - Specify a value from 0 - 7.</li> </ul>                                                                                                                                                                                                                                                                                                                                       |
| source-port <0-65535>               | Configures the protocol source port to match. The source protocol can be TCP, UDP or any other protocol identified by its number (<0-255>). <ul style="list-style-type: none"> <li>&lt;0-65535&gt; - Specify the source port from 0 - 65535.</li> </ul>                                                                                                                                                                                                               |
| source-port-bitmark <0-65535>       | Configures the decimal number representing the protocol source port bits to match <ul style="list-style-type: none"> <li>&lt;0-65535&gt; - Specify the source port bits from 0 - 65535.</li> </ul>                                                                                                                                                                                                                                                                    |
| rule-precedence <1-128>             | The following keywords are recursive and common to all of the above parameters: <ul style="list-style-type: none"> <li>rule-precedence - Assigns a precedence to this permit rule <ul style="list-style-type: none"> <li>&lt;1-128&gt; - Specify a value from 1 - 5000.</li> </ul> </li> </ul> <p><b>Note:</b> Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 4 and is applied first to packets.</p> |

### Usage Guidelines

Use this command to permit traffic between networks/hosts based on the protocol type selected in the access list configuration. The following protocols are supported:

- TCP
- UDP
- <0-255> (any Internet protocol other than TCP, UDP, and ICMP)

Packet content is checked against the ACEs in the ACL, and are allowed or denied access based on the ACL configuration.

- Filtering TCP/UDP allows you to specify port numbers as filtering criteria.

## Examples

The following example permits outgoing TCP packets from all sources within the 192.168.14.0 network to any destination, with the TCP control flag set to 16 (acknowledge):

```
nx9500-6C8809(config-ip-ex3500-ext-acl-test)#permit tcp 192.168.14.0/24 any control-flag
16 rule-precedence 2
nx9500-6C8809(config-ip-ex3500-ext-acl-test)#show context
ip ex3500-ext-access-list test
 deny tcp 192.168.14.0/24 host 192.168.13.13 rule-precedence 1
 permit tcp 192.168.14.0/24 any control-flag 16 rule-precedence 2
nx9500-6C8809(config-ip-ex3500-ext-acl-test)#
```

## Related Commands

|                                     |                                                                                     |
|-------------------------------------|-------------------------------------------------------------------------------------|
| <code>no (ex3500-ext acl)</code> on | Removes a specified permit access rule from this IPv4 EX3500 extended ACL page 1423 |
|-------------------------------------|-------------------------------------------------------------------------------------|

*no (ex3500-ext acl)*

Removes a deny or permit access rule from this IPv4 EX3500 extended ACL

## Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
no [deny|permit] [<0-255>|tcp|udp] [<SOURCE-NETWORK-IP/MASK>|any|host <SOURCE-HOST-IP>]
[<DEST-NETWORK-IP/MASK>|any|host <DEST-HOST-IP>] [control-flag <0-63>|destination-port
<0-65535>|
destination-port-bitmark <0-65535>|dscp <0-63>|ex3500-time-range <TIME-RANGE-NAME>|
ip-precedence <0-63>|rule-precedence <1-128>|source-port <0-65535>|source-port-bitmark
<0-65535>]
```

## Parameters

no <PARAMETERS>

|                                    |                                                                     |
|------------------------------------|---------------------------------------------------------------------|
| <code>no &lt;PARAMETERS&gt;</code> | Removes a deny or permit access rule based on the parameters passed |
|------------------------------------|---------------------------------------------------------------------|

## Usage Guidelines

The keyword 'control-flag <0-63>' is only applicable to ACL rules filtering TCP traffic.

## Examples

The following example shows the IPv4 EX3500 extended ACL 'test' settings before the 'no' commands are executed:

```
nx9500-6C8809(config-ip-ex3500-ext-acl-test)#show context
ip ex3500-ext-access-list test
 deny tcp 192.168.14.0/24 host 192.168.13.13 rule-precedence 1
 permit tcp 192.168.14.0/24 any control-flag 16 rule-precedence 2
nx9500-6C8809(config-ip-ex3500-ext-acl-test)#
nx9500-6C8809(config-ip-ex3500-ext-acl-test)#no permit tcp 192.168.14.0/24 any control-
flag 16 rule-precedence 2
```

The following example shows the IPv4 EX3500 extended ACL 'test' settings after the 'no' commands are executed:

```
nx9500-6C8809(config-ip-ex3500-ext-acl-test)#show context
ip ex3500-ext-access-list test
 deny tcp 192.168.14.0/24 host 192.168.13.13 rule-precedence 1
nx9500-6C8809(config-ip-ex3500-ext-acl-test)#
```

## ex3500-std-access-list

An EX3500 standard ACL is a policy-based ACL that contains a set of filter criteria and action that is applied to traffic originating from a specified source.

The following table summarizes IPv4 EX3500 standard ACL configuration commands:

**Table 40: EX3500-Standard-Access-List-Config Commands**

| Command                                              | Description                                                                                                                                                                                                              |
|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">deny (ex3500-std acl)</a> on page 1424   | Creates a deny rule that rejects packets from a specified source or sources. The source can be a single device or a range of devices within a specified network. Use this command to also edit an existing deny rule.    |
| <a href="#">permit (ex3500-std acl)</a> on page 1425 | Creates a permit rule that allows packets from a specified source or sources. The source can be a single device or a range of devices within a specified network. Use this command to also edit an existing permit rule. |
| <a href="#">no (ex3500-std acl)</a> on page 1426     | Removes a deny and/or a permit access rule from this IPv4 EX3500 extended ACL                                                                                                                                            |



### Note

To implement the EX3500 standard ACL, apply it directly to a EX35XX device, or to an EX35XX profile. For more information, see [access-group](#) on page 1299.

### *deny (ex3500-std acl)*

Creates a deny rule that rejects packets from a specified source or sources. The source can be a single device or a range of devices within a specified network. Use this command to also edit an existing deny rule.

#### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
deny [<SOURCE-NETWORK-IP/MASK>|any|host <SOURCE-HOST-IP>] {ex3500-time-range <TIME-RANGE-NAME>}
```

#### Parameters

```
deny [<SOURCE-NETWORK-IP/MASK>|any|host <SOURCE-HOST-IP>] {ex3500-time-range <TIME-RANGE-NAME>}
```

|                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| deny [<SOURCE-NETWORK-IP/MASK> any host <SOURCE-HOST-IP>] | <p>Creates a deny rule that rejects packets from a specified source or a network. Use one of the following options to specify the source: any, host, or network.</p> <ul style="list-style-type: none"> <li>• &lt;SOURCE-NETWORK-IP/MASK&gt; - Configures a network as the source. Provide the network's IPv4 address along with the mask.</li> <li>• host &lt;SOURCE-HOST-IP&gt; - Configures a single device as the source. Provide the host device's IPv4 address.</li> <li>• any - Specifies that the source can be any device</li> </ul> |
| ex3500-time-range <TIME-RANGE-NAME>                       | <p>Optional. Applies a periodic or absolute time range to this deny rule</p> <ul style="list-style-type: none"> <li>• &lt;TIME-RANGE-NAME&gt; - Specify the time range name (should be existing and configured). The ACL is triggered during the time period configured in the specified EX3500 time range. For information on configuring EX3500 time-range, see <a href="#">ex3500</a>.</li> </ul>                                                                                                                                          |

### Examples

```

nx9500-6C8809(config-ip-ex3500-std-acl-test)#deny 192.168.14.0/24
nx9500-6C8809(config-ip-ex3500-std-acl-test)#show context
ip ex3500-std-access-list test
 deny 192.168.13.0/24
nx9500-6C8809(config-ip-ex3500-std-acl-test)#

```

### Related Commands

|                                                  |                                                                         |
|--------------------------------------------------|-------------------------------------------------------------------------|
| <a href="#">no (ex3500-std acl)</a> on page 1426 | Removes a specified deny access rule from this IPv4 EX3500 standard ACL |
|--------------------------------------------------|-------------------------------------------------------------------------|

### *permit (ex3500-std acl)*

Creates a permit rule that allows packets from a specified source or sources. The source can be a single device or a range of devices within a specified network. Use this command to also edit an existing permit rule.

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
permit [<SOURCE-NETWORK-IP/MASK>|any|host <SOURCE-HOST-IP>] {ex3500-time-range <TIME-RANGE-NAME>}
```

### Parameters

```
permit [<SOURCE-NETWORK-IP/MASK>|any|host <SOURCE-HOST-IP>] {ex3500-time-range <TIME-RANGE-NAME>}
```

|                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>permit [&lt;SOURCE-NETWORK-IP/MASK&gt; any host &lt;SOURCE-HOST-IP&gt;]</pre> | <p>Creates a permit rule that allows packets from a specified source or a network. Use one of the following options to specify the source: any, host, or network.</p> <ul style="list-style-type: none"> <li>• &lt;SOURCE-NETWORK-IP/MASK&gt; – Configures a network as the source. Provide the network’s IPv4 address along with the mask.</li> <li>• host &lt;SOURCE-HOST-IP&gt; – Configures a single device as the source. Provide the host device’s IPv4 address.</li> <li>• any – Specifies that the source can be any device</li> </ul> |
| <pre>ex3500-time-range &lt;TIME-RANGE-NAME&gt;</pre>                               | <p>Optional. Applies a periodic or absolute time range to this permit rule</p> <ul style="list-style-type: none"> <li>• &lt;TIME-RANGE-NAME&gt; – Specify the time range name (should be existing and configured). The ACL is triggered during the time period configured in the specified EX3500 time range. For information on configuring EX3500 time-range, see <a href="#">ex3500</a>.</li> </ul>                                                                                                                                         |

### Examples

```
nx9500-6C8809(config-ip-ex3500-std-acl-test)#permit host 192.168.13.13 ex3500-time-range EX3500_TimeRange_01
nx9500-6C8809(config-ip-ex3500-std-acl-test)#show contextnx9500-6C8809(config-ip-ex3500-std-acl-test)#show context
ip ex3500-std-access-list test
deny 192.168.14.0/24
permit host 192.168.13.13 ex3500-time-range EX3500_TimeRange_01
nx9500-6C8809(config-ip-ex3500-std-acl-test)#
nx9500-6C8809(config-ip-ex3500-std-acl-test)#
```

### Related Commands

|                                   |                                                                                            |
|-----------------------------------|--------------------------------------------------------------------------------------------|
| <pre>no (ex3500-std acl) on</pre> | <p>Removes a specified permit access rule from this IPv4 EX3500 standard ACL page 1426</p> |
|-----------------------------------|--------------------------------------------------------------------------------------------|

*no (ex3500-std acl)*

Removes a deny or permit access rule from this IPv4 EX3500 standard ACL

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
no [deny|permit] [<SOURCE-IP/MASK>|any|host <IP>] {ex3500-time-range <TIME-RANGE-NAME>}
```

### Parameters

```
no <PARAMETERS>
```

|                                  |                                                                            |
|----------------------------------|----------------------------------------------------------------------------|
| <pre>no &lt;PARAMETERS&gt;</pre> | <p>Removes a deny or permit access rule based on the parameters passed</p> |
|----------------------------------|----------------------------------------------------------------------------|

### Examples

The following example shows the IPv4 EX3500 standard ACL ‘test’ settings before the ‘no’ commands are executed:

```
nx9500-6C8809(config-ip-ex3500-std-acl-test)#show context
ip ex3500-std-access-list test
```

---

```
deny 192.168.14.0/24
permit host 192.168.13.13 ex3500-time-range EX3500_TimeRange_01
nx9500-6C8809(config-ip-ex3500-std-acl-test)#
nx9500-6C8809(config-ip-ex3500-std-acl-test)#no deny 192.168.14.0/24
```

The following example shows the IPv4 EX3500 standard ACL 'test' settings after the 'no' commands are executed:

```
nx9500-6C8809(config-ip-ex3500-std-acl-test)#show context
ip ex3500-std-access-list test
permit host 192.168.13.13 ex3500-time-range EX3500_TimeRange_01
nx9500-6C8809(config-ip-ex3500-std-acl-test)#
```

# DHCP POLICY

## DHCP-SERVER-POLICY

---

This chapter summarizes DHCP (Dynamic Host Control Protocol) server policy commands in the CLI command structure.

DHCP automatically assigns network IP addresses to requesting clients to enable them access to network resources. DHCP tracks IP address assignments, their lease times and their availability. Each subnet can be configured with its own address pool. Whenever a DHCP client requests an IP address, the DHCP server assigns an IP address from that subnet's address pool. When the controller's (wireless controller, service platform, or access point) onboard DHCP server allocates an address to a DHCP client, the client is assigned a lease, which expires after a pre-determined interval. Before a lease expires, wireless clients (with assigned leases) are expected to renew them to continue using the addresses. Once the lease expires, the client is no longer permitted to use the leased IP address. The controller's DHCP server policy ensures all IP addresses are unique, and no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). IP address management is conducted by a controller's DHCP server and not by an administrator.

The controller's internal DHCP server groups wireless clients based on defined user-class option values. Clients with a defined set of user class values are segregated by class. A DHCP server can associate multiple classes to each pool. Each class in a pool is assigned an exclusive range of IP addresses. DHCP clients are compared against classes. If the client matches one of the classes assigned to the pool, it receives an IP address from the range assigned to the class. If the client doesn't match any of the classes in the pool, it receives an IP address from a default pool range (if defined). Multiple IP addresses for a single VLAN allow the configuration of multiple IP addresses, each belonging to different subnet. Class configuration allows a DHCP client to obtain an address from the first pool to which the class is assigned.

Use the (config) instance to configure DHCP/DHCPv6 server policy parameters. To navigate to the config DHCP server policy instance, use the following commands:

```
<DEVICE> (config)#dhcp-server-policy <POLICY-NAME>
nx9500-6C8809(config)#dhcp-server-policy test
nx9500-6C8809(config-dhcp-server-policy-test)#?
DHCP policy Mode commands:
 bootp BOOTP specific configuration
 dhcp-class Configure DHCP class (for address allocation using DHCP
 user-class options)
 dhcp-pool Configure DHCP server address pool
 dhcp-server Activating dhcp server based on criteria
 no Negate a command or set its defaults
 option Define DHCP server option
 ping Specify ping parameters used by DHCP Server

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
```



```

service Service Commands
show Show running system information
write Write running configuration to memory or terminal

```

```
nx9500-6C8809(config-dhcp-policy-test)#
```

To navigate to the config DHCPv6 server policy instance, use the following commands:

```

<DEVICE>(config)#dhcpv6-server-policy <POLICY-NAME>
nx9500-6C8809(config)#dhcpv6-server-policy test
nx9500-6C8809(config-dhcpv6-server-policy-test)#?

```

DHCPv6 server policy Mode commands:

```

dhcpv6-pool Configure DHCPV6 server address pool
no Negate a command or set its defaults
option Define DHCPV6 server option
restrict-vendor-options Restrict vendor specific options to be sent in
 server reply
server-preference Server preference value sent in the reply, by the
 server to client

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

```

```
nx9500-6C8809(config-dhcpv6-server-policy-test)#
```

This chapter is organized into the following subsections:

- [dhcp-server-policy commands](#) on page 1429.
- [dhcpv6-server-policy commands](#) on page 1471.

## dhcp-server-policy commands

The following table summarizes the DHCP server policy configuration mode commands:

**Table 41: DHCP-Server-Policy Config Mode Commands**

| Command                                                                | Description                                |
|------------------------------------------------------------------------|--------------------------------------------|
| <a href="#">bootp (dhcpv4-server-policy-config)</a> on page 1430       | Configures a BOOTP specific configuration  |
| <a href="#">dhcp-class (dhcpv4-server-policy-config)</a> on page 1431  | Configures a DHCP server class             |
| <a href="#">dhcp-pool (dhcpv4-server-policy-config)</a> on page 1434   | Configures a DHCP server address pool      |
| <a href="#">dhcp-server (dhcpv4-server-policy-config)</a> on page 1469 | Configures DHCP server options             |
| <a href="#">option (dhcpv4-server-policy-config)</a> on page 1468      | Defines the DHCP option used in DHCP pools |

**Table 41: DHCP-Server-Policy Config Mode Commands (continued)**

| Command                                                      | Description                                     |
|--------------------------------------------------------------|-------------------------------------------------|
| <code>ping (dhcpv4-server-policy-config)</code> on page 1468 | Specifies ping parameters used by a DHCP server |
| <code>no (dhcpv4-server-policy-config)</code> on page 1471   |                                                 |



**Note**

For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see [COMMON COMMANDS](#) on page 640.



**Note**

The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (\_) character. In other words, the name of a device cannot contain an underscore.

*bootp (dhcpv4-server-policy-config)*

Configures a BOOTP specific configuration

BOOTP (Bootstrap Protocol) requests are used by UNIX diskless workstations to obtain the location of their boot image and IP address within the managed network. A BOOTP configuration server provides this information and also assigns an IP address from a configured pool of IP addresses. By default, all BOOTP requests are forwarded to the BOOTP configuration server by the controller. When enabled, this feature allows controllers, using this DHCP server policy, to ignore BOOTP requests.

**Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

**Syntax**

`bootp ignore`

**Parameters**

`bootp ignore`

|                           |                                              |
|---------------------------|----------------------------------------------|
| <code>bootp ignore</code> | Enables controllers to ignore BOOTP requests |
|---------------------------|----------------------------------------------|

**Examples**

```
nx9500-6C8809(config-dhcp-policy-test)#bootp ignore
nx9500-6C8809(config-dhcp-policy-test)#show context
dhcp-server-policy test
 bootp ignore
nx9500-6C8809(config-dhcp-policy-test)#
```

## Related Commands

`no (dhcpv4-server-policy-config)` on page 1471

Disables the ignore BOOTP requests option

### *dhcp-class (dhcpv4-server-policy-config)*

Creates a DHCP server class and enters its configuration mode. Use this command to configure or modify user class option values. Once defined, the controller's internal DHCP server uses the configured values to group wireless clients into DHCP classes, such that each user class consists of wireless clients sharing the same set of user class values.

A controller, service platform, or access point's local DHCP server assigns IP addresses to requesting DHCP clients based on user class option names. The DHCP server can assign IP addresses from as many IP address ranges as defined by an administrator. The DHCP user class associates a particular range of IP addresses to a device in such a way that all devices of that type are assigned IP addresses from the defined range.

A DHCP user class applies different DHCP settings to a set of wireless clients. Wireless clients using the same DHCP settings are grouped under one DHCP class. Grouping users into classes facilitates the provision of differentiated service.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
dhcp-class <DHCP-CLASS-NAME>
```

### Parameters

```
dhcp-class <DHCP-CLASS-NAME>
```

|                   |                                                                                                                                                                                                                                                                                                                |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <DHCP-CLASS-NAME> | Creates a DHCP user class <ul style="list-style-type: none"><li>• &lt;DHCP-CLASS-NAME&gt; - Specify a name that appropriately identifies this class of wireless clients. If a class with the specified name does not exist, it is created. The class name should not exceed 32 characters in length.</li></ul> |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

Use the `dhcp-class` command to configure a DHCP user class.

```
nx9500-6C8809(config-dhcp-policy-test)#dhcp-class dhcpclass1
nx9500-6C8809(config-dhcp-policy-test-class-dhcpclass1)#?
DHCP class Mode commands:
 multiple-user-class Enable multiple user class option
 no Negate a command or set its defaults
 option Configure DHCP Server options

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
```

```

help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

```

```
nx9500-6C8809(config-dhcp-policy-test-class-dhcpclass1)#
```

The following table summarizes the DHCP user class configuration commands.

**Table 42: DHCP-User-Class Config Mode Commands**

| Command                                                                                     | Description                                                                    |
|---------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| <code>multiple-user-class (dhcpv4-class-config)</code> on page 1432                         | Enables or disables multiple user class option for this DHCP user class policy |
| <code>option (dhcpv4-class-config)</code> on page 1433                                      | Configures DHCP user class options for this DHCP user class policy             |
| <code>no (dhcpv4-class-config)</code> on page 1433                                          | Removes this DHCP class settings                                               |
| <code>no (dhcpv4-server-policy-config)</code> on page 1471 (dhcp-server-policy-config-mode) | Removes this DHCP class from the DHCP server policy                            |

### multiple-user-class (dhcpv4-class-config)

Enables multiple user class option for this DHCP user class policy. Enabling this option allows this user class to transmit multiple option values to other DHCP servers also supporting multiple user class options.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
multiple-user-class
```

#### Parameters

None

#### Examples

```

nx9500-6C8809(config-dhcp-policy-test-class-class1)#multiple-user-class
nx9500-6C8809(config-dhcp-policy-test-class-dhcpclass1)#show context
dhcp-class dhcpclass1
 multiple-user-class
nx9500-6C8809(config-dhcp-policy-test-class-dhcpclass1)#

```

#### Related Commands

|                                                    |                                                                                 |
|----------------------------------------------------|---------------------------------------------------------------------------------|
| <code>no (dhcpv4-class-config)</code> on page 1433 | Disables the multiple user class option for the selected DHCP user class policy |
|----------------------------------------------------|---------------------------------------------------------------------------------|

### option (dhcpv4-class-config)

Configures DHCP user class options for this DHCP user class policy

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
option user-class <VALUE>
```

Parameters

```
option user-class <VALUE>
```

|                    |                                                                                                                                                        |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| user-class <VALUE> | Configures DHCP user class options <ul style="list-style-type: none"><li>• &lt;VALUE&gt; - Specify the DHCP user class option's ASCII value.</li></ul> |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|

Examples

```
nx9500-6C8809(config-dhcp-policy-test-class-class1)#option user-class test
nx9500-6C8809(config-dhcp-policy-test-class-dhcpclass1)#show context
dhcp-class dhcpclass1
 option user-class test
 multiple-user-class
nx9500-6C8809(config-dhcp-policy-test-class-dhcpclass1)#
```

Related Commands

|                                                       |                                               |
|-------------------------------------------------------|-----------------------------------------------|
| <a href="#">no (dhcpv4-class-config)</a> on page 1433 | Removes the configured DHCP user class option |
|-------------------------------------------------------|-----------------------------------------------|

### no (dhcpv4-class-config)

Removes this DHCP user class policy's settings

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
no [multiple-user-class|option]
no option user-class <VALUE>
```

Parameters

```
no <PARAMETERS>
```

|                 |                                                                     |
|-----------------|---------------------------------------------------------------------|
| no <PARAMETERS> | Disables multiple user class options on this DHCP user class policy |
|-----------------|---------------------------------------------------------------------|

Examples

The following example shows the DHCP class settings before the 'no' commands are executed:

```
nx9500-6C8809(config-dhcp-policy-test-class-dhcpclass1)#show context
dhcp-class dhcpclass1
 option user-class test
```

```

multiple-user-class
nx9500-6C8809(config-dhcp-policy-test-class-dhcpclass1)#
nx9500-6C8809(config-dhcp-policy-test-class-class1)#no multiple-user-class
nx9500-6C8809(config-dhcp-policy-test-class-dhcpclass1)#no option user-class test

```

The following example shows the DHCP class settings after the 'no' commands are executed:

```

nx9500-6C8809(config-dhcp-policy-test-class-dhcpclass1)#show context
dhcp-class dhcpclass1
nx9500-6C8809(config-dhcp-policy-test-class-dhcpclass1)#

```

### *dhcp-pool (dhcpv4-server-policy-config)*

Creates a DHCP server address pool and enters its configuration mode.

The DHCP pool command creates and manages a pool of IP addresses. These IP addresses are assigned to devices using the DHCP protocol. IP addresses have to be unique for each device in the network. Since IP addresses are finite, DHCP ensures that every device, in the network, is issued a unique IP address by tracking the issue, release, and reissue of IP addresses.

The DHCP pool command configures a finite set of IP addresses that can be assigned whenever a device joins a network.

DHCP services are available for specific IP interfaces. A pool (or range) of IP network addresses and DHCP options can be created for each IP interface defined. This range of addresses is available to DHCP enabled wireless devices on either a permanent or leased basis. This enables the reuse of limited IP address resources for deployment in any network. DHCP options are provided to each DHCP client with a DHCP response and provides DHCP clients information required to access network resources (default gateway, domain name, DNS server and WINS server configuration). An option exists to identify the vendor and functionality of a DHCP client. The information is a variable-length string of characters (or octets) with a meaning specified by the vendor of the DHCP client.

#### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### **Syntax**

```
dhcp-pool <POOL-NAME>
```

#### **Parameters**

```
dhcp-pool <POOL-NAME>
```

|             |                                                                                                                                                                                                                                                                                                                                                                         |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <POOL-NAME> | <p>Creates a DHCP server address pool</p> <ul style="list-style-type: none"> <li>• &lt;POOL-NAME&gt; - Specify a name that appropriately identifies this DHCP address pool. If a pool with the specified name does not exist, it is created. The pool name cannot be modified as part of the edit process. However, an obsolete address pool can be deleted.</li> </ul> |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### **Examples**

Use the `dhcp-pool` command to configure a DHCP user pool.

```

nx9500-6C8809(config-dhcp-policy-test)#dhcp-pool pool1
nx9500-6C8809(config-dhcp-policy-test-pool-pool1)#?

```

DHCP pool Mode commands:

```

address Configure network pool's included addresses
bootfile Boot file name
ddns Dynamic DNS Configuration
default-router Default routers
dns-server DNS Servers
domain-name Configure domain-name
excluded-address Prevent DHCP Server from assigning certain addresses
lease Address lease time
netbios-name-server NetBIOS (WINS) name servers
netbios-node-type NetBIOS node type
network Network on which DHCP server will be deployed
next-server Next server in boot process
no Negate a command or set its defaults
option Raw DHCP options
respond-via-unicast Send DHCP offer and DHCP Ack as unicast messages
static-binding Configure static address bindings
static-route Add static routes to be installed on dhcp clients
update Control the usage of DDNS service

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

```

nx9500-6C8809(config-dhcp-policy-test-pool-pool1)#

The following table summarizes the DHCP user pool configuration commands.

**Table 43: DHCP-User-Pool Config Mode Commands**

|                                                                       |                                                                                                                                            |
|-----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">address (dhcpv4-pool-config)</a> on page 1436             | Specifies a range of addresses for a DHCP address pool                                                                                     |
| <a href="#">bootfile (dhcpv4-pool-config)</a> on page 1437            | Assigns a bootfile name. The bootfile name can contain letters, numbers, dots and hyphens. Consecutive dots and hyphens are not permitted. |
| <a href="#">ddns (dhcpv4-pool-config)</a> on page 1438                | Configures dynamic DNS parameters                                                                                                          |
| <a href="#">default-router (dhcpv4-pool-config)</a> on page 1439      | Configures a default router or gateway IP address for the network pool                                                                     |
| <a href="#">dns-server (dhcpv4-pool-config)</a> on page 1440          | Sets a DNS server's IP address available to all DHCP clients connected to the DHCP pool                                                    |
| <a href="#">domain-name (dhcpv4-pool-config)</a> on page 1442         | Sets the domain name for the network pool                                                                                                  |
| <a href="#">excluded-address (dhcpv4-pool-config)</a> on page 1442    | Prevents a DHCP server from assigning certain addresses to the DHCP pool                                                                   |
| <a href="#">lease (dhcpv4-pool-config)</a> on page 1444               | Sets a valid lease for the IP address used by DHCP clients in the DHCP pool                                                                |
| <a href="#">netbios-name-server (dhcpv4-pool-config)</a> on page 1445 | Configures a NetBIOS (WINS) name server's IP address                                                                                       |
| <a href="#">netbios-node-type (dhcpv4-pool-config)</a> on page 1446   | Defines the NetBIOS node type                                                                                                              |

**Table 43: DHCP-User-Pool Config Mode Commands (continued)**

|                                                                    |                                                                   |
|--------------------------------------------------------------------|-------------------------------------------------------------------|
| <code>network (dhcpv4-pool-config)</code> on page 1446             | Configures the network on which the DHCP server is deployed       |
| <code>next-server (dhcpv4-pool-config)</code> on page 1447         | Configures the next server in the boot process                    |
| <code>option (dhcpv4-pool-config)</code> on page 1448              | Configures RAW DHCP options                                       |
| <code>respond-via-unicast (dhcpv4-pool-config)</code> on page 1449 | Sends a DHCP offer and DHCP Ack as unicast messages               |
| <code>static-route (dhcpv4-pool-config)</code> on page 1450        | Configures a static route for a DHCP pool                         |
| <code>update (dhcpv4-pool-config)</code> on page 1450              | Controls the usage of the DDNS service                            |
| <code>static-binding (dhcpv4-pool-config)</code> on page 1455      | Configures static address bindings                                |
| <code>no (dhcpv4-pool-static-binding)</code> on page 1467          | Removes this DHCP pool settings or reverts them to default values |

### address (dhcpv4-pool-config)

Adds IP addresses to the DHCP address pool. These IP addresses are assigned to each device joining the network.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
address [<IP> | <HOST-ALIAS-NAME> | range]
address [<IP> | <HOST-ALIAS-NAME> | range [<START-IP> | <START-HOST-ALIAS-NAME>] [<END-IP> | <END-
HOST-ALIAS-NAME>]]
{ class <DHCP-CLASS-NAME> }
```

#### Parameters

```
address [<IP> | <HOST-ALIAS-NAME> | range [<START-IP> | <START-HOST-ALIAS-NAME>] [<END-IP> | <END-
HOST-ALIAS-NAME>]]
{ class <DHCP-CLASS-NAME> }
```

|                   |                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IP>              | Adds a single IP address to the DHCP address pool                                                                                                                                                                                                                                                                                                                                     |
| <HOST-ALIAS-NAME> | Adds a single host mapped to the specified host alias. The host alias should be existing and configured.<br><br><b>Note:</b> A network host alias maps a name to a single network host. For example, 'alias host \$HOST 1.1.1.100'. In this example the host alias is '\$HOST' and it maps to a single host '1.1.1.100'. For more information, see <a href="#">alias</a> on page 237. |



|                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| range [<START-IP> <START-HOST-ALIAS-NAME>] [<END-IP> <END-HOST-ALIAS-NAME>] | <p>Adds a range of IP addresses to the DHCP address pool. Use one of the following options to provide the first IP address in the range:</p> <ul style="list-style-type: none"> <li>• &lt;START-IP&gt; – Specifies the first IP address in the range</li> <li>• &lt;START-HOST-ALIAS-NAME&gt; – Specifies a host alias, mapped to the first IP address in the range</li> </ul> <p>Use one of the following options to provide the last IP address in the range:</p> <ul style="list-style-type: none"> <li>• &lt;END-IP&gt; – Specifies the last IP address in the range</li> <li>• &lt;END-HOST-ALIAS-NAME&gt; – Specifies a host alias, mapped to the last IP address in the range</li> </ul> <p><b>Note:</b> The host aliases should be existing and configured.</p> |
| class <DHCP-CLASS-NAME>                                                     | <p>Optional. Applies additional DHCP options, or a modified set of options to those available to wireless clients. For more information, see <a href="#">dhcp-class (dhcpv4-server-policy-config)</a> on page 1431.</p> <ul style="list-style-type: none"> <li>• &lt;DHCP-CLASS-NAME&gt; – Sets the DHCP class (should be existing and configured)</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                           |

### Examples

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#address 192.168.13.4 class dhcpclass1
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
 address 192.168.13.4 class dhcpclass1
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

### Related Commands

|                                                                       |                                                                                 |
|-----------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <a href="#">no (dhcpv4-pool-static-binding)</a> on page 1467          | Removes the DHCP pool's configured IP addresses                                 |
| <a href="#">dhcp-class (dhcpv4-server-policy-config)</a> on page 1431 | Creates and configures the DHCP class parameters                                |
| <a href="#">alias</a> on page 237                                     | Creates and configures network, VLAN, host, string, and network-service aliases |

## bootfile (dhcpv4-pool-config)

The Bootfile command provides a diskless node path to the image file while booting up. Only one file can be configured for each DHCP pool.

For more information on the BOOTP protocol with reference to the DHCP policy, see bootp [bootp \(dhcpv4-server-policy-config\)](#) on page 1430.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
bootfile <IMAGE-FILE-PATH>
```

### Parameters

```
bootfile <IMAGE-FILE-PATH>
```

|                   |                                                                                                                                                                  |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IMAGE-FILE-PATH> | Sets the path to the boot image for BOOTP clients. The file name can contain letters, numbers, dots and hyphens. Consecutive dots and hyphens are not permitted. |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#bootfile test.txt
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
 address 192.168.13.4 class dhcpclass1
 bootfile test.txt
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

#### Related Commands

|                                                                  |                                                  |
|------------------------------------------------------------------|--------------------------------------------------|
| <a href="#">no</a> on page 1451                                  | Resets the boot image path for the BOOTP clients |
| <a href="#">bootp (dhcpv4-server-policy-config)</a> on page 1430 | Configures BOOTP protocol parameters             |

### ddns (dhcpv4-pool-config)

DDNS (Dynamic DNS) parameters. Dynamic DNS provides a way to access an individual device in a DHCP serviced network using a static device name.

Depending on the DHCP server's configuration, the IP address of a device changes periodically. To ensure continuous accessibility to a device (having a dynamic IP address), the device's current IP address is published to a DDNS server that resolves the static device name (used to access the device) with a changing IP address.

The DDNS server must be accessible from outside the network and must be configured as an address resolver.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
ddns [domainname|multiple-user-class|server|ttl]
ddns domainname <DDNS-DOMAIN-NAME>
ddns multiple-user-class
ddns server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
ddns ttl <1-864000>
```

#### Parameters

```
ddns domainname <DDNS-DOMAIN-NAME>
```

|                    |                                                                                                                                                                                                                                                                                                     |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| domainname         | Sets the domain name used for DNS updates                                                                                                                                                                                                                                                           |
| <DDNS-DOMAIN-NAME> | The controller uses DNS to convert human readable host names into IP addresses. Host names are not case sensitive and can contain alphabetic or numeric letters or a hyphen. A FQDN (fully qualified domain name) consists of a host name plus a domain name. For example, computername.domain.com. |

```
ddns multiple-user-class
```

|                     |                                                               |
|---------------------|---------------------------------------------------------------|
| multiple-user-class | Enables the multiple user class options with this DDNS domain |
|---------------------|---------------------------------------------------------------|

```
ddns server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| server                     | Configures the DDNS server used by this DHCP profile                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| [<IP> <HOST-ALIAS-NAME>]   | Configures the primary DDNS server. This is the default server. Use one of the following options to specify the primary DDNS server: <ul style="list-style-type: none"> <li>• &lt;IP&gt; – Specifies the primary DDNS server’s IP address</li> <li>• &lt;HOST-ALIAS-NAME&gt; – Specifies a host alias, mapped to the primary DDNS server’s IP address. The host alias should be existing and configured.</li> </ul> <p><b>Note:</b> A network host alias maps a name to a single network host. For example, ‘alias host \$HOST 1.1.1.100’. In this example the host alias is ‘\$HOST’ and it maps to a single host ‘1.1.1.100’. For more information, see <a href="#">alias</a> on page 237.</p> |
| {<IP1> <HOST-ALIAS-NAME1>} | Optional. Configures the secondary DDNS server. If the primary server is not reachable, this server is used. Use one of the following options to identify the secondary DDNS server: <ul style="list-style-type: none"> <li>• &lt;IP&gt; – Specifies the secondary DDNS server’s IP address</li> <li>• &lt;HOST-ALIAS-NAME&gt; – Specifies a host alias, mapped to the secondary DDNS server’s IP address. The host alias should be existing and configured.</li> </ul>                                                                                                                                                                                                                          |

```
ddns ttl <1-864000>
```

|                |                                                                                                                                                                        |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ttl <1-864000> | Configures the TTL (Time To Live) value for DDNS updates <ul style="list-style-type: none"> <li>• &lt;1-86400&gt; – Specify a value from 1- 864000 seconds.</li> </ul> |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#ddns domainname WID
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#ddns multiple-user-class
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#ddns server 192.168.13.9
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
address 192.168.13.4 class dhcpclass1
 ddns server 192.168.13.9
 ddns domainname WID
 ddns multiple-user-class
bootfile test.txt
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

### Related Commands

|                                 |                                                |
|---------------------------------|------------------------------------------------|
| <a href="#">no</a> on page 1451 | Resets or disables a DHCP pool’s DDNS settings |
|---------------------------------|------------------------------------------------|

## default-router (dhcpv4-pool-config)

Configures a default router or gateway IP address for the network pool

After a DHCP client has booted, the client begins sending packets to its default router. Set the IP address of one or a group of routers the controller uses to map host names into IP addresses available to DHCP supported clients. Up to 8 default router IP addresses are supported.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
default-router [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

#### Parameters

```
default-router [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [<IP> <HOST-ALIAS-NAME>]   | <p>Configures the primary default router, using one of the following options:</p> <ul style="list-style-type: none"> <li>• &lt;IP&gt; - Specifies the primary default router's IP address</li> <li>• &lt;HOST-ALIAS-NAME&gt; - Specifies a host alias, mapped to the primary default router's IP address. The host alias should be existing and configured.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                  |
| {<IP1> <HOST-ALIAS-NAME1>} | <p>Optional. Configures the secondary default router, using one of the following options:</p> <ul style="list-style-type: none"> <li>• &lt;IP1&gt; - Specifies the secondary default router's IP address</li> <li>• &lt;HOST-ALIAS-NAME1&gt; - Specifies a host alias, mapped to the secondary default router's IP address. If the primary default router is unavailable, the secondary router is used.</li> </ul> <p><b>Note:</b> A network host alias maps a name to a single network host. For example, 'alias host \$HOST 1.1.1.100'. In this example the host alias is '\$HOST' and it maps to a single host '1.1.1.100'. For more information, see <a href="#">alias</a> on page 237 .</p> <p><b>Note:</b> A maximum of 8 default routers can be configured..</p> |

#### Usage Guidelines

The IP address of the router should be on the same subnet as the client subnet.

#### Examples

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#default-router 192.168.13.8
192.168.13.9
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
 address 192.168.13.4 class dhcpclass1
 ddns server 192.168.13.9
 ddns domainname WID
 ddns multiple-user-class
 bootfile test.txt
 default-router 192.168.13.8 192.168.13.9
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

#### Related Commands

|                                 |                                     |
|---------------------------------|-------------------------------------|
| <a href="#">no</a> on page 1451 | Removes the default router settings |
|---------------------------------|-------------------------------------|

### dns-server (dhcpv4-pool-config)

Configures a network's DNS server. The DNS server supports all clients connected to networks supported by the DHCP server.

For DHCP clients, the DNS server's IP address maps the hostname to an IP address. DHCP clients use the DNS server's IP address based on the order (sequence) configured.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
dns-server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

#### Parameters

```
dns-server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

|                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>[&lt;IP&gt; &lt;HOST-ALIAS-NAME&gt;]</p>   | <p>Configures the primary DNS server, using one of the following options:</p> <ul style="list-style-type: none"><li>• &lt;IP&gt; – Specifies the primary DNS server’s IP address</li><li>• &lt;HOST-ALIAS-NAME&gt; – Specifies a host alias, mapped to the primary DNS server’s IP address</li></ul> <p><b>Note:</b> A maximum of 8 DNS server’s can be configured.</p> <p>To enable redirection of DNS queries to OpenDNS it is necessary that the DNS server IP addresses provided here should point to the OpenDNS resolver (208.67.220.220 or 208.67.222.222). OpenDNS is a proxy DNS server that provides additional functionality, such as Web filtering, reporting, and performance enhancements in addition to DNS services. When configured on a WLAN, DNS queries from wireless clients are redirected to OpenDNS. The following example illustrates the configuration:</p> <pre>dhcp-server-policy dhcppolicy   dhcp-pool dhcppool     network 192.168.1.0/24     address range 192.168.1.160 192.168.1.200     default-router 192.168.1.105     dns-server 208.67.220.220</pre> <p>Note, the above example shows the OpenDNS server as being 208.67.220.220. The alternative IP address 208.67.222.222 can also be used.</p> <p>For more information on the entire configuration that needs to be done to integrate WiNG access point, controllers, and service platform with OpenDNS, see <a href="#">opendns (user and privi exec modes)</a> on page 86.</p> |
| <p>{&lt;IP1&gt; &lt;HOST-ALIAS-NAME1&gt;}</p> | <p>Optional. Configures the secondary DNS server, using one of the following options:</p> <ul style="list-style-type: none"><li>• &lt;IP1&gt; – Specifies the secondary DNS server’s IP address</li><li>• &lt;HOST-ALIAS-NAME1&gt; – Specifies a host alias, mapped to the secondary DNS server’s IP address. If the primary DNS server is unavailable, the secondary server is used.</li></ul> <p><b>Note:</b> A network host alias maps a name to a single network host. For example, ‘alias host \$HOST 1.1.1.100’. In this example the host alias is ‘\$HOST’ and it maps to a single host ‘1.1.1.100’. For more information, see <a href="#">alias</a> on page 237.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

#### Examples

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#dns-server 192.168.13.19
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
 address 192.168.13.4 class dhcpclass1
 ddns server 192.168.13.9
 ddns domainname WID
 ddns multiple-user-class
 bootfile test.txt
 default-router 192.168.13.8 192.168.13.9
```

```
dns-server 192.168.13.19
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands

|                 |                             |
|-----------------|-----------------------------|
| no on page 1451 | Removes DNS server settings |
|-----------------|-----------------------------|

### domain-name (dhcpv4-pool-config)

Sets the domain name for the DHCP pool. This is the domain name used by the controller with this pool.

Domain names are not case sensitive and can contain alphabetic or numeric letters or a hyphen. The FQDN consists of the host name and the domain name. For example, computername.domain.com.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
domain-name <DOMAIN-NAME>
```

Parameters

```
domain-name <DOMAIN-NAME>
```

|               |                                     |
|---------------|-------------------------------------|
| <DOMAIN-NAME> | Defines the DHCP pool's domain name |
|---------------|-------------------------------------|

Examples

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#domain-name documentation
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
 address 192.168.13.4 class dhcpclass1
 ddns server 192.168.13.9
 ddns domainname WID
 ddns multiple-user-class
 domain-name documentation
 bootfile test.txt
 default-router 192.168.13.8 192.168.13.9
 dns-server 192.168.13.19
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands

|                 |                                   |
|-----------------|-----------------------------------|
| no on page 1451 | Removes a DHCP pool's domain name |
|-----------------|-----------------------------------|

### excluded-address (dhcpv4-pool-config)

Identifies a single IP address or a range of IP addresses, included in the DHCP address pool, that cannot be assigned to clients by the DHCP server

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000

- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
excluded-address [<IP> | <HOST-ALIAS-NAME>] range]
excluded-address <IP>
excluded-address <HOST-ALIAS-NAME>
excluded-address range [<START-IP> | <START-HOST-ALIAS-NAME>] [<END-IP> | <END-HOST-ALIAS-NAME>]
```

### Parameters

```
excluded-address <IP>
```

|      |                                                      |
|------|------------------------------------------------------|
| <IP> | Adds a single IP address to the exclude address list |
|------|------------------------------------------------------|

```
excluded-address <HOST-ALIAS-NAME>
```

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <HOST-ALIAS-NAME> | <p>Adds a host alias. The host alias is mapped to a host's IP address. The host identified by the host alias is added to the excluded address list. The host alias should be existing and configured.</p> <p><b>Note:</b> A network host alias maps a name to a single network host. For example, 'alias host \$HOST 1.1.1.100'. In this example the host alias is '\$HOST' and it maps to a single host '1.1.1.100'. For more information, see <a href="#">alias</a> on page 237.</p> |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
excluded-address [<START-IP> | <START-HOST-ALIAS-NAME>] [<END-IP> | <END-HOST-ALIAS-NAME>]
```

|                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>range [ &lt;START-IP&gt;   &lt;START-HOST-ALIAS-NAME&gt; ] [ &lt;END-IP&gt;   &lt;END-HOST-ALIAS-NAME&gt; ]</pre> | <p>Adds a range of IP addresses to the excluded address list. Use one of the following options to provide the first IP address in the range:</p> <ul style="list-style-type: none"> <li>• &lt;START-IP&gt; - Specifies the first IP address in the range</li> <li>• &lt;START-HOST-ALIAS-NAME&gt; - Specifies a host alias, mapped to the first IP address in the range</li> </ul> <p>Use one of the following options to provide the last IP address in the range:</p> <ul style="list-style-type: none"> <li>• &lt;END-IP&gt; - Specifies the last IP address in the range</li> <li>• &lt;END-HOST-ALIAS-NAME&gt; - Specifies a host alias, mapped to the last IP address in the range</li> </ul> <p>The host aliases should be existing and configured.</p> |
|------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#excluded-address range 192.168.13.25 192.168.13.28
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
network 192.168.13.0/24
address 192.168.13.4 class dhcpclass1
ddns server 192.168.13.9
ddns domainname WID
ddns multiple-user-class
excluded-address range 192.168.13.25 192.168.13.28
domain-name documentation
bootfile test.txt
default-router 192.168.13.8 192.168.13.9
dns-server 192.168.13.19
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

### Related Commands

|                                 |                                           |
|---------------------------------|-------------------------------------------|
| <a href="#">no</a> on page 1451 | Removes the exclude IP addresses settings |
|---------------------------------|-------------------------------------------|

## lease (dhcpv4-pool-config)

A lease is the duration a DHCP issued IP address is valid. Once a lease expires, and if the lease is not renewed, the IP address is revoked and is available for reuse. Generally, before an IP lease expires, the client tries to get the same IP address issued for the next lease period. This feature is enabled by default, with a lease period of 24 hours (1 day).

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
lease [<0-365>|infinite]
lease infinite
lease <0-365> {<0-23>} {<0-59>} {<0-59>}
```

### Parameters

```
lease infinite
```

|          |                                                                   |
|----------|-------------------------------------------------------------------|
| infinite | The lease never expires (equal to a static IP address assignment) |
|----------|-------------------------------------------------------------------|

```
lease <0-365> {<0-23>} {<0-59>} {<0-59>}
```

|         |                                                                                                                        |
|---------|------------------------------------------------------------------------------------------------------------------------|
| <0-365> | Configures the lease duration in days<br><b>Note:</b> Days may be 0 only when hours and/or minutes are greater than 0. |
| <0-23>  | Optional. Sets the lease duration in hours                                                                             |
| <0-59>  | Optional. Sets the lease duration in minutes                                                                           |
| <0-59>  | Optional. Sets the lease duration in seconds                                                                           |

### Usage Guidelines

If lease parameter is not configured on the DHCP pool, the default is used. The default is 24 hours.

### Examples

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#lease 100 23 59 59
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
network 192.168.13.0/24
address 192.168.13.4 class dhcpclass1
lease 100 23 59 59
ddns server 192.168.13.9
ddns domainname WID
ddns multiple-user-class
excluded-address range 192.168.13.25 192.168.13.28
domain-name documentation
bootfile test.txt
default-router 192.168.13.8 192.168.13.9
dns-server 192.168.13.19
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

### Related Commands

|                 |                                                        |
|-----------------|--------------------------------------------------------|
| no on page 1451 | Resets values or disables the DHCP pool lease settings |
|-----------------|--------------------------------------------------------|



## netbios-name-server (dhcpv4-pool-config)

Configures the NetBIOS (WINS) name server's IP address. This server is used to resolve NetBIOS host names.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
netbios-name-server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

### Parameters

```
netbios-name-server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [<IP> <HOST-ALIAS-NAME>]   | Configures the primary NetBIOS name server, using one of the following options: <ul style="list-style-type: none"><li>• &lt;IP&gt; – Specifies the primary NetBIOS name server's IP address</li><li>• &lt;HOST-ALIAS-NAME&gt; – Specifies a host alias, mapped to the primary NetBIOS name server's IP address</li></ul>                                                                                                                                                                                                                                                                                                                                                                                  |
| {<IP1> <HOST-ALIAS-NAME1>} | Optional. Configures the secondary NetBIOS name server, using one of the following options: <ul style="list-style-type: none"><li>• &lt;IP1&gt; – Specifies the secondary NetBIOS name server's IP address</li><li>• &lt;HOST-ALIAS-NAME1&gt; – Specifies a host alias, mapped to the secondary NetBIOS name server's IP address. If the primary NetBIOS name server is unavailable, the secondary server is used.</li></ul> <p><b>Note:</b> A network host alias maps a name to a single network host. For example, 'alias host \$HOST 1.1.1.100'. In this example the host alias is '\$HOST' and it maps to a single host '1.1.1.100'. For more information, see <a href="#">alias</a> on page 237.</p> |

### Examples

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#netbios-name-server 192.168.13.25
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
 network 192.168.13.0/24
 address 192.168.13.4 class dhcpclass1
 lease 100 23 59 59
 ddns server 192.168.13.9
 ddns domainname WID
 ddns multiple-user-class
 excluded-address range 192.168.13.25 192.168.13.28
 domain-name documentation
 bootfile test.txt
 default-router 192.168.13.8 192.168.13.9
 dns-server 192.168.13.19
 netbios-name-server 192.168.13.25
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

### Related Commands

|                                 |                                          |
|---------------------------------|------------------------------------------|
| <a href="#">no</a> on page 1451 | Removes the NetBIOS name server settings |
|---------------------------------|------------------------------------------|

## netbios-node-type (dhcpv4-pool-config)

Defines the predefined NetBIOS node type. The NetBIOS node type resolves NetBIOS names to IP addresses.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
netbios-node-type [b-node|h-node|m-node|p-node]
```

Parameters

```
netbios-node-type [b-node|h-node|m-node|p-node]
```

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [b-node h-node m-node p-node] | Defines the netbios node type                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|                               | <ul style="list-style-type: none"><li>• b-node – Sets the node type as broadcast. Uses broadcasts to query nodes on the network for the owner of a NetBIOS name.</li><li>• h-node – Sets the node type as hybrid. Uses a combination of two or more nodes.</li><li>• m-node – Sets the node type as mixed. A mixed node uses broadcasted queries to find a node, and failing that, queries a known p-node name server for the address.</li><li>• p-node – Sets the node type as peer-to-peer. Uses directed calls to communicate with a known NetBIOS name server (such as a WINS server), for the IP address of a NetBIOS machine.</li></ul> |

Examples

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#netbios-node-type b-node
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
 network 192.168.13.0/24
 address 192.168.13.4 class dhcpclass1
 lease 100 23 59 59
 ddns server 192.168.13.9
 ddns domainname WID
 ddns multiple-user-class
 excluded-address range 192.168.13.25 192.168.13.28
 domain-name documentation
 netbios-node-type b-node
 bootfile test.txt
 default-router 192.168.13.8 192.168.13.9
 dns-server 192.168.13.19
 netbios-name-server 192.168.13.25
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands

|                 |                                        |
|-----------------|----------------------------------------|
| no on page 1451 | Removes the NetBIOS node type settings |
|-----------------|----------------------------------------|

## network (dhcpv4-pool-config)

Configures the DHCP server's network settings

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533

- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

`network` [`<IP/M>` | `<NETWORK-ALIAS-NAME>`]

#### Parameters

`network` [`<IP/M>` | `<NETWORK-ALIAS-NAME>`]

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;IP/M&gt;</code>               | Configures the network number and mask (for example, 192.168.13.0/24)                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <code>&lt;NETWORK-ALIAS-NAME&gt;</code> | <p>Configures a network alias to identify the network number and mask</p> <ul style="list-style-type: none"> <li>• <code>&lt;NETWORK-ALIAS-NAME&gt;</code> - Specify the network alias name. It should be existing and configured.</li> </ul> <p><b>Note:</b> A network alias defines a single network address. For example, 'alias network \$NET 1.1.0/24'. In this example, the network alias name is: \$NET, and the network it is mapped to is: 1.1.0/24. For more information, see <a href="#">alias</a> on page 237.</p> |

#### Examples

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#network 192.168.13.0/24
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
 network 192.168.13.0/24
 address 192.168.13.4 class dhcpclass1
 lease 100 23 59 59
 ddns server 192.168.13.9
 ddns domainname WID
 ddns multiple-user-class
 excluded-address range 192.168.13.25 192.168.13.28
 domain-name documentation
 netbios-node-type b-node
 bootfile test.txt
 default-router 192.168.13.8 192.168.13.9
 dns-server 192.168.13.19
 netbios-name-server 192.168.13.25
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

#### Related Commands

|                              |                                                                   |
|------------------------------|-------------------------------------------------------------------|
| <code>no</code> on page 1451 | Removes the network number and mask configured for this DHCP pool |
|------------------------------|-------------------------------------------------------------------|

### next-server (dhcpv4-pool-config)

Configures the next server in the boot process

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

`next-server` [`<IP>` | `<HOST-ALIAS-NAME>`]

#### Parameters

`next-server` [`<IP>` | `<HOST-ALIAS-NAME>`]

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IP>              | Configures the next server's (the first server in the boot process) IP address                                                                                                                                                                                                                                                                                                                                                                                                               |
| <HOST-ALIAS-NAME> | <p>Configures a host alias, mapped to the next server's IP address</p> <ul style="list-style-type: none"> <li>• &lt;HOST-ALIAS-NAME&gt; – Specify the host alias name. It should be existing and configured.</li> </ul> <p><b>Note:</b> A host alias maps a name to a single network host. For example, 'alias host \$HOST 1.1.1.100'. In this example the host alias is '\$HOST' and it maps to a single host '1.1.1.100'. For more information, see <a href="#">alias</a> on page 237.</p> |

### Examples

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#next-server 192.168.13.26
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
 network 192.168.13.0/24
 address 192.168.13.4 class dhcpclass1
 lease 100 23 59 59
 ddns server 192.168.13.9
 ddns domainname WID
 ddns multiple-user-class
 excluded-address range 192.168.13.25 192.168.13.28
 domain-name documentation
 netbios-node-type b-node
 bootfile test.txt
 default-router 192.168.13.8 192.168.13.9
 dns-server 192.168.13.19
 netbios-name-server 192.168.13.25
 next-server 192.168.13.26
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

### Related Commands

|                                 |                                                |
|---------------------------------|------------------------------------------------|
| <a href="#">no</a> on page 1451 | Removes the next server configuration settings |
|---------------------------------|------------------------------------------------|

### option (dhcpv4-pool-config)

Configures raw DHCP options. The DHCP option must be configured under the DHCP server policy. The options configured under the DHCP pool/DHCP server policy can also be used in static-bindings.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
option <OPTION-NAME> [<DHCP-OPTION-IP> | <DHCP-OPTION-ASCII>]
```

#### Parameters

```
option <OPTION-NAME> [<DHCP-OPTION-IP> | <DHCP-OPTION-ASCII>]
```

|                     |                                     |
|---------------------|-------------------------------------|
| <OPTION-NAME>       | Sets the name of the DHCP option    |
| <DHCP-OPTION-IP>    | Sets DHCP option as an IP address   |
| <DHCP-OPTION-ASCII> | Sets DHCP option as an ASCII string |



#### Note

An option name in ASCII format accepts a backslash (\) as an input, but is not displayed in the output. Use the **show > running > config** command to view the output. Use a double backslash to represent a single backslash.

#### Examples

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#option option1 157.235.208.80
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
address 192.168.13.4 class dhcpclass1
ddns server 192.168.13.9
ddns multiple-user-class
excluded-address range 192.168.13.25 192.168.13.28
netbios-node-type b-node
dns-server 192.168.13.19
netbios-name-server 192.168.13.25
option option1 157.235.208.80
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

#### Related Commands

|                        |                                                         |
|------------------------|---------------------------------------------------------|
| <b>no</b> on page 1451 | Resets values or disables the DHCP pool option settings |
|------------------------|---------------------------------------------------------|

### respond-via-unicast (dhcpv4-pool-config)

Sends DHCP offer and acknowledgment as unicast messages

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
respond-via-unicast
```

#### Parameters



#### Note

None

#### Examples

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#respond-via-unicast
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
address 192.168.13.4 class dhcpclass1
ddns server 192.168.13.9
ddns multiple-user-class
excluded-address range 192.168.13.25 192.168.13.28
netbios-node-type b-node
dns-server 192.168.13.19
```

```

netbios-name-server 192.168.13.25
option option1 157.235.208.80
respond-via-unicast
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#

```

#### Related Commands

**no** on page 1451 Disables sending of a DHCP offer and DHCP Ack as unicast messages. When disabled, sends offer and acknowledgment as broadcast messages.

### static-route (dhcpv4-pool-config)

Configures a static route for a DHCP pool. Static routes define a gateway for traffic intended for other networks. This gateway is always used when an IP address does not match any route in the network.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
static-route <IP/M> <IP>
```

#### Parameters

```
static-route <IP/M> <IP>
```

|        |                                                               |
|--------|---------------------------------------------------------------|
| <IP/M> | Specifies the IP destination prefix (for example, 10.0.0.0/8) |
| <IP>   | Specifies the gateway IP address                              |

#### Examples

```

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#static-route 192.168.13.0/24
192.168.13.7
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
 address 192.168.13.4 class dhcpclass1
 ddns server 192.168.13.9
 ddns multiple-user-class
 excluded-address range 192.168.13.25 192.168.13.28
 netbios-node-type b-node
 dns-server 192.168.13.19
 netbios-name-server 192.168.13.25
 option option1 157.235.208.80
 respond-via-unicast
 static-route 192.168.13.0/24 192.168.13.7
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#

```

#### Related Commands

**no** on page 1451 Removes static route settings

### update (dhcpv4-pool-config)

Controls the use of the DDNS service

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
update dns {override}
```

#### Parameters

```
update dns {override}
```

|                           |                                                                                                                                                                 |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>dns {override}</pre> | Configures DDNS parameters <ul style="list-style-type: none"> <li>• <code>override</code> - Optional. Enables DDNS updates on an onboard DHCP server</li> </ul> |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Usage Guidelines

A DHCP client cannot perform updates for RR's A, TXT and PTR resource records. Use `update (dns) (override)` to enable the internal DHCP server to send DDNS updates for resource records. The DHCP server can override the client, even if the client is configured to perform the updates.

In the DHCP server's DHCP pool, FQDN is configured as the DDNS domain name. This is used internally in DHCP packets between the DHCP server and the DNS server.

#### Examples

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#update dns override
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
 address 192.168.13.4 class dhcpclass1
 update dns override
 ddns server 192.168.13.9
 ddns multiple-user-class
 excluded-address range 192.168.13.25 192.168.13.28
 netbios-node-type b-node
 dns-server 192.168.13.19
 netbios-name-server 192.168.13.25
 option option1 157.235.208.80
 respond-via-unicast
 static-route 192.168.13.0/24 192.168.13.7
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

#### Related Commands

|               |                                                  |
|---------------|--------------------------------------------------|
| <pre>no</pre> | on page 1451 Removes dynamic DNS service control |
|---------------|--------------------------------------------------|

#### **no**

Removes or resets this DHCP user pool's settings

Supported in the following platforms:

- Access Points — AP 6522, AP 6532, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 81XX, AP 8232
- Wireless Controllers — RFS 4000, RFS 6000
- Service Platforms — NX 7500, NX 9500, NX 9510

## Syntax

```
no [address|bootfile|ddns|default-router|dns-server|domain-name|excluded-address|
 lease|netbios-name-server|netbios-node-type|network|next-server|option|
 respond-via-unicast|static-binding|static-route|update]
no [bootfile|default-router|dns-server|domain-name|lease|netbios-name-server|
 netbios-node-type|next-server|network|respond-via-unicast]
no address [<IP>|<HOST-ALIAS-NAME>|all]
no address range [<START-IP>|<START-HOST-ALIAS-NAME>] [<END-IP>|<END-HOST-ALIAS-NAME>]
no ddns [domainname|multiple-user-class|server|ttl]
no excluded-address [<IP>|<HOST-ALIAS-NAME>]
no excluded-address range [<START-IP>|<START-HOST-ALIAS-NAME>] [<END-IP>|<END-HOST-ALIAS-
NAME>]
no option <OPTION-NAME>
no static-binding client-identifier <CLIENT-IDENTIFIER>
no static-binding hardware-address <MAC>
no static-route <IP/MASK> <GATEWAY-IP>
no update dns {override}
```

## Parameters

```
no [bootfile|default-router|dns-server|domain-name|lease|netbios-name-server|
netbios-node-type|next-server|network|respond-via-unicast]
```

|                        |                                                             |
|------------------------|-------------------------------------------------------------|
| no bootfile            | Removes a BOOTP bootfile configuration                      |
| no default-router      | Removes the configured default router for the DHCP pool     |
| no dns-server          | Removes the configured DNS server for the DHCP pool         |
| no domain-name         | Removes the configured DNS domain name                      |
| no lease               | Resets the lease to its default (24 hours)                  |
| no netbios-name-server | Removes the configured NetBIOS name server                  |
| no netbios-node-type   | Removes the NetBIOS node type                               |
| no next-server         | Removes the next server utilized in the boot process        |
| no network             | Removes the DHCP server network information                 |
| no respond-via-unicast | Sets the DHCP offer and ACK as broadcast instead of unicast |

```
no address [<IP>|<HOST-ALIAS-NAME>|all]
```

|                   |                                                                                                       |
|-------------------|-------------------------------------------------------------------------------------------------------|
| no address        | Resets configured DHCP pool addresses                                                                 |
| <IP>              | Removes an IP address from the list of addresses                                                      |
| <HOST-ALIAS-NAME> | Removes the host alias (used to identify a single host) associated with this DHCP pool's address list |
| all               | Removes configured DHCP IP addresses                                                                  |

```
no address range [<START-IP>|<START-HOST-ALIAS-NAME>] [<END-IP>|<END-HOST-ALIAS-NAME>]
```



|                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| no address                                                                  | Resets the DHCP pool addresses                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| range [<START-IP> <START-HOST-ALIAS-NAME>] [<END-IP> <END-HOST-ALIAS-NAME>] | <p>Removes a range of IP addresses and host aliases associated with this DHCP pool's address list.</p> <ul style="list-style-type: none"> <li>• &lt;START-IP&gt; – Specify the first IP address in the range.</li> <li>• &lt;START-HOST-ALIAS-NAME&gt; – Specify the host alias, mapped to the first IP address in the range.</li> <li>• &lt;END-IP&gt; – Specify the last IP address in the range.</li> <li>• &lt;END-HOST-ALIAS-NAME&gt; – Specify the host alias, mapped to the last IP address in the range.</li> </ul> <p><b>Note:</b> The specified IP addresses and host aliases are removed from the DHCP pool's address list.</p> |

no ddns [domainname|multiple-user-class|server|ttl]

|                     |                                                       |
|---------------------|-------------------------------------------------------|
| no ddns             | Resets DDNS parameters                                |
| domainname          | Removes DDNS domain name information                  |
| multiple-user-class | Resets the use of a multiple user class with the DDNS |
| server              | Removes configured DDNS servers                       |
| ttl                 | Resets the TTL information for DDNS updates           |

no excluded-address [<IP>|HOST-ALIAS-NAME>]

|                          |                                                                                                                                                                                                    |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| no excluded-address <IP> | <p>Removes an excluded IP address from the list of addresses that cannot be issued by the DHCP server</p> <ul style="list-style-type: none"> <li>• &lt;IP&gt; – Specify the IP address.</li> </ul> |
| <HOST-ALIAS-NAME>        | Removes the host alias (used to identify a single host) associated with this DHCP pool's excluded-address list                                                                                     |

no no excluded-address range [<START-IP>|<START-HOST-ALIAS-NAME>] [<END-IP>|<END-HOST-ALIAS-NAME>]

|                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| no excluded-address                                                         | Removes a range of excluded IP addresses from the list of addresses that cannot be issued by the DHCP server                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| range [<START-IP> <START-HOST-ALIAS-NAME>] [<END-IP> <END-HOST-ALIAS-NAME>] | <p>Removes a range of IP addresses and host aliases associated with this DHCP pool's excluded address list.</p> <ul style="list-style-type: none"> <li>• &lt;START-IP&gt; – Specify the first IP address in the range.</li> <li>• &lt;START-HOST-ALIAS-NAME&gt; – Specify the host alias, mapped to the first IP address in the range.</li> <li>• &lt;END-IP&gt; – Specify the last IP address in the range.</li> <li>• &lt;END-HOST-ALIAS-NAME&gt; – Specify the host alias, mapped to the last IP address in the range.</li> <li>• <b>Note:</b> The specified IP addresses and host aliases are removed from the DHCP pool's excluded address list</li> </ul> |

no option <OPTION-NAME>

|               |                                |
|---------------|--------------------------------|
| no option     | Resets DHCP option information |
| <OPTION-NAME> | Defines the DHCP option        |

no static-binding client-identifier <CLIENT-IDENTIFIER>

|                                       |                                                                                                                                                     |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| no static-binding                     | Removes static bindings for DHCP client                                                                                                             |
| client-identifier <CLIENT-IDENTIFIER> | Resets client identifier information <ul style="list-style-type: none"> <li>• &lt;CLIENT-IDENTIFIER&gt; - Specify the client identifier.</li> </ul> |

no static-binding hardware-address <MAC>

|                        |                                                                                                                                                      |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| no static-binding      | Removes static bindings for a DHCP client                                                                                                            |
| hardware-address <MAC> | Resets information based on the hardware address <ul style="list-style-type: none"> <li>• &lt;MAC&gt; - Specify the hardware MAC address.</li> </ul> |

no static-route <IP/MASK> <GATEWAY-IP>

|                 |                                                                                |
|-----------------|--------------------------------------------------------------------------------|
| no static-route | Removes static routes for this DHCP pool                                       |
| <IP/MASK>       | Removes routing information for a particular subnet                            |
| <GATEWAY-IP>    | Removes the gateway information from a particular subnet's routing information |

no update dns {*override*}

|               |                                                                                                                |
|---------------|----------------------------------------------------------------------------------------------------------------|
| no update dns | Removes DDNS settings                                                                                          |
| override      | <ul style="list-style-type: none"> <li>• Optional. Removes DDNS updates from an onboard DHCP server</li> </ul> |

## Examples

The following example shows the DHCP pool settings before the 'no' commands are executed:

```
<exsw5>(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
 network 192.168.13.0/24
 address 192.168.13.4 class dhcpclass1
 lease 100 23 59 59
 ddns server 192.168.13.9
 ddns domainname WID
 ddns multiple-user-class
 excluded-address range 192.168.13.25 192.168.13.28
 domain-name documentation
 netbios-node-type b-node
 bootfile test.txt
 default-router 192.168.13.8 192.168.13.9
 dns-server 192.168.13.19
 netbios-name-server 192.168.13.25
 next-server 192.168.13.26
<exsw5>(config-dhcp-policy-test-pool-testPool)#
<exsw5>(config-dhcp-policy-test-pool-testPool)#no bootfile
<exsw5>(config-dhcp-policy-test-pool-testPool)#no network
<exsw5>(config-dhcp-policy-test-pool-testPool)#no default-router
<exsw5>(config-dhcp-policy-test-pool-testPool)#no next-server
<exsw5>(config-dhcp-policy-test-pool-testPool)#no domain-name
```

```

<exsw5>(config-dhcp-policy-test-pool-testPool)#no ddns domainname
<exsw5>(config-dhcp-policy-test-pool-testPool)#no lease
The following example shows the DHCP pool settings after the 'no' commands are executed:
<exsw5>(config-dhcp-policy-test-pool-testPool)#show context
dhcp-pool testPool
 address 192.168.13.4 class dhcpclass1
 ddns server 192.168.13.9
 ddns multiple-user-class
 excluded-address range 192.168.13.25 192.168.13.28
 netbios-node-type b-node
 dns-server 192.168.13.19
 netbios-name-server 192.168.13.25
<exsw5>(config-dhcp-policy-test-pool-testPool)#

```

#### Related Commands

|                            |                                                      |
|----------------------------|------------------------------------------------------|
| <b>address</b>             | Configures the DHCP server's IP address pool         |
| <b>bootfile</b>            | Configures the BOOTP boot file path                  |
| <b>ddns</b>                | Configures DDNS for use with this DHCP pool          |
| <b>default-router</b>      | Configures default routers for this DHCP pool        |
| <b>dns-server</b>          | Configures default DNS servers for this DHCP pool    |
| <b>domain-name</b>         | Configures the DDNS domain name for this DHCP pool   |
| <b>excluded-address</b>    | Configures IP addresses assigned as static addresses |
| <b>lease</b>               | Configures the DHCP lease settings                   |
| <b>netbios-name-server</b> | Configures the NetBIOS name server                   |
| <b>netbios-node-type</b>   | Configures the NetBIOS node type                     |
| <b>network</b>             | Configures the DHCP server's network settings        |
| <b>next-server</b>         | Configures the next server in the BOOTP boot process |
| <b>option</b>              | Configures the DHCP option                           |
| <b>respond-via-unicast</b> | Configures how a DHCP request and ACK are sent       |
| <b>static-binding</b>      | Configure static binding information                 |
| <b>static-route</b>        | Configures static routes installed on DHCP clients   |
| <b>update</b>              | Controls DDNS service usage                          |

#### **static-binding (dhcpv4-pool-config)**

Configures static IP address information for a particular device. Static address binding is executed on the device's hostname, client identifier, or MAC address. Static bindings allow the configuration of client parameters, such as DHCP server, DNS server, default routers, fixed IP address, etc.

A static address binding is a collection of configuration parameters, including an IP address, associated with, or bound to, a DHCP client. Bindings are managed by DHCP servers. DHCP bindings automatically map a device MAC address to an IP address using a pool of DHCP supplied addresses. Static bindings assign IP addresses without creating numerous host pools with manual bindings. Static host bindings use a text file the DHCP server reads. It eliminates the need for a lengthy configuration file and reduces the space required to maintain address pools.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
static-binding [client-identifier <CLIENT>|hardware-address <MAC>]
```

### Parameters

```
static-binding [client-identifier <CLIENT>|hardware-address <MAC>]
```

|                               |                                                                                                                                                                                                                                                           |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| client-identifier<br><CLIENT> | Enables a static binding configuration for a client based on its client identifier (as provided by DHCP option 61 and its key value) <ul style="list-style-type: none"> <li>• &lt;CLIENT&gt; - Specify the client identifier (DHCP option 61).</li> </ul> |
| hardware-address<br><MAC>     | Enables a static binding configuration for a client based on its MAC address <ul style="list-style-type: none"> <li>• &lt;MAC&gt; - Specify the MAC address of the client.</li> </ul>                                                                     |

### Examples

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#static-binding client-identifier test
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
```

```
dhcp-pool testPool
address 192.168.13.4 class dhcpclass1
update dns override
ddns server 192.168.13.9
ddns multiple-user-class
excluded-address range 192.168.13.25 192.168.13.28
netbios-node-type b-node
dns-server 192.168.13.19
netbios-name-server 192.168.13.25
option option1 157.235.208.80
respond-via-unicast
static-route 192.168.13.0/24 192.168.13.7
```

#### **static-binding client-identifier test**

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
rfs4000-229D58(config-dhcp-policy-test-pool-testPool-binding-test)#?
```

#### DHCP static binding Mode commands:

```
bootfile Boot file name
client-name Client name
default-router Default routers
dns-server DNS Servers
domain-name Configure domain-name
ip-address Fixed IP address for host
netbios-name-server NetBIOS (WINS) name servers
netbios-node-type NetBIOS node type
next-server Next server in boot process
no Negate a command or set its defaults
option Raw DHCP options
respond-via-unicast Send DHCP offer and DHCP Ack as unicast messages
static-route Add static routes to be installed on dhcp clients
```

```
clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal
```

```

rfs4000-229D58(config-dhcp-policy-test-pool-testPool-binding-test)#
nx9500-6C8809(config-dhcp-policy-test-pool-pool1)#static-binding hardware-address
11-22-33-44-55-66
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-11-22-33-44-55-66)#?
DHCP static binding Mode commands:
 bootfile Boot file name
 client-name Client name
 default-router Default routers
 dns-server DNS Servers
 domain-name Configure domain-name
 ip-address Fixed IP address for host
 netbios-name-server NetBIOS (WINS) name servers
 netbios-node-type NetBIOS node type
 next-server Next server in boot process
 no Negate a command or set its defaults
 option Raw DHCP options
 respond-via-unicast Send DHCP offer and DHCP Ack as unicast messages
 static-route Add static routes to be installed on dhcp clients

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-11-22-33-44-55-66)#

```

The following table summarizes the DHCPv4-User-Pool Static Binding commands:

**Table 44: DHCPv4-User-Pool Static-Binding  
Config Mode Commands**

| Command                                                                       | Description                                                                               |
|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| <a href="#">bootfile (dhcpv4-pool-static-binding)</a> on page 1458            | Assigns a Bootfile name for the DHCP configuration on the network pool                    |
| <a href="#">client-name (dhcpv4-pool-static-binding)</a> on page 1458         | Configures a client name                                                                  |
| <a href="#">default-router (dhcpv4-pool-static-binding)</a> on page 1459      | Configures default router or gateway IP address                                           |
| <a href="#">dns-server (dhcpv4-pool-static-binding)</a> on page 1460          | Sets the DNS server's IP address available to all DHCP clients connected to the DHCP pool |
| <a href="#">domain-name (dhcpv4-pool-static-binding)</a> on page 1461         | Sets the network pool's domain name                                                       |
| <a href="#">ip-address (dhcpv4-pool-static-binding)</a> on page 1462          | Configures a host's fixed IP address                                                      |
| <a href="#">netbios-name-server (dhcpv4-pool-static-binding)</a> on page 1462 | Configures a NetBIOS (WINS) name server IP address                                        |
| <a href="#">netbios-node-type (dhcpv4-pool-static-binding)</a> on page 1463   | Defines the NetBIOS node type                                                             |
| <a href="#">next-server (dhcpv4-pool-static-binding)</a> on page 1464         | Specifies the next server used in the boot process                                        |
| <a href="#">option (dhcpv4-pool-static-binding)</a> on page 1465              | Configures raw DHCP options                                                               |

**Table 44: DHCPv4-User-Pool Static-Binding Config Mode Commands (continued)**

| Command                                                                       | Description                                                            |
|-------------------------------------------------------------------------------|------------------------------------------------------------------------|
| <a href="#">respond-via-unicast (dhcpv4-pool-static-binding)</a> on page 1466 | Sends a DHCP offer and DHCP Ack as unicast messages                    |
| <a href="#">static-route (dhcpv4-pool-static-binding)</a> on page 1466        | Adds static routes installed on DHCP clients                           |
| <a href="#">no (dhcpv4-pool-static-binding)</a> on page 1467                  | Negates or reverts to default this DHCP Pool's static binding settings |

[no \(dhcpv4-pool-static-binding\)](#) on page 1467  
bootfile (dhcpv4-pool-static-binding)

The Bootfile command provides a diskless node the path to the image file used while booting up. Only one file can be configured for each static IP binding.

For more information on the BOOTP protocol with reference to static binding, see [bootp \(dhcpv4-server-policy-config\)](#) on page 1430.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
bootfile <IMAGE-FILE-PATH>
```

#### Parameters

```
bootfile <IMAGE-FILE-PATH>
```

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IMAGE-FILE-PATH>> | Sets the path to the boot image for BOOTP file used with this user pool. The file name can contain letters, numbers, dots and hyphens. Consecutive dots and hyphens are not permitted. Boot files (Boot Protocol) can be used to boot remote systems over the network. BOOTP messages are encapsulated inside UDP messages so requests and replies can be forwarded. Each DHCP network pool can use a different file as needed. |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#bootfile test.txt
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#show context
 static-binding client-identifier test
 bootfile test.txt
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#
```

#### Related Commands

|                                                                  |                                                             |
|------------------------------------------------------------------|-------------------------------------------------------------|
| <a href="#">bootp (dhcpv4-server-policy-config)</a> on page 1430 | Configures BOOTP protocol parameters                        |
| <a href="#">no (dhcpv4-pool-static-binding)</a> on page 1467     | Resets values or disables DHCP pool static binding settings |

client-name (dhcpv4-pool-static-binding)

Configures the name of the client requesting DHCP Server support

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
client-name <NAME>
```

#### Parameters

```
client-name <NAME>
```

<NAME> Specify the name of the client using this static IP address host pool. Do not include the domain name.

#### Examples

```
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#client-name test
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#show context
static-binding client-identifier test
 client-name test
 bootfile test.txt
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#
```

#### Related Commands

|                                                              |                                     |
|--------------------------------------------------------------|-------------------------------------|
| <a href="#">no (dhcpv4-pool-static-binding)</a> on page 1467 | Removes the name of the DHCP client |
|--------------------------------------------------------------|-------------------------------------|

#### default-router (dhcpv4-pool-static-binding)

Configures a default router or gateway IP address for the static binding configuration. After a DHCP client has booted, the client begins sending packets to its default router.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
default-router [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

#### Parameters

```
default-router [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [<IP> <HOST-ALIAS-NAME>]   | <p>Configures the primary default router, using one of the following options:</p> <ul style="list-style-type: none"> <li>• &lt;IP&gt; – Specifies the primary default router’s IP address</li> <li>• &lt;HOST-ALIAS-NAME&gt; – Specifies a host alias, mapped to the primary default router’s IP address</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| {<IP1> <HOST-ALIAS-NAME1>} | <p>Optional. Configures the secondary default router, using one of the following options:</p> <ul style="list-style-type: none"> <li>• &lt;IP1&gt; – Specifies the secondary default router’s IP address</li> <li>• &lt;HOST-ALIAS-NAME1&gt; – Specifies a host alias, mapped to the secondary default router’s IP address. If the primary default router is unavailable, the secondary router is used.</li> </ul> <p><b>Note:</b> A network host alias maps a name to a single network host. For example, ‘alias host \$HOST 1.1.1.100’. In this example the host alias is ‘\$HOST’ and it maps to a single host ‘1.1.1.100’. For more information, see <a href="#">alias</a> on page 237.</p> <p><b>Note:</b> A maximum of 8 default routers can be configured..</p> |

### Usage Guidelines

The IP address of the router should be on the same subnet as the client subnet.

### Examples

```

nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#default-router 172.16.10.8
172.16.10.9
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#show context
static-binding client-identifier test
client-name RFID
bootfile test.txt
default-router 172.16.10.8 172.16.10.9
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#

```

### Related Commands

|                                                              |                                     |
|--------------------------------------------------------------|-------------------------------------|
| <a href="#">no (dhcpv4-pool-static-binding)</a> on page 1467 | Removes the default router settings |
|--------------------------------------------------------------|-------------------------------------|

## dns-server (dhcpv4-pool-static-binding)

Configures a network’s DNS server. The DNS server supports all clients for which static binding has been configured.

For this client, the DNS server’s IP address maps the host name to an IP address. DHCP clients use the DNS server’s IP address based on the order (sequence) configured.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
dns-server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

### Parameters

```
dns-server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```



|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [<IP> <HOST-ALIAS - NAME>] | <ul style="list-style-type: none"> <li>Configures the primary DNS server, using one of the following options:</li> <li>&lt;IP&gt; – Specifies the primary DNS server’s IP address</li> <li>&lt;HOST-ALIAS-NAME&gt; – Specifies a host alias, mapped to the primary DNS server’s IP address</li> </ul>                                                                                                                                                                                                                                                                                                                                                           |
| {<IP1> <HOST-ALIAS-NAME1>} | <p>Optional. Configures the secondary DNS server, using one of the following options:</p> <ul style="list-style-type: none"> <li>&lt;IP1&gt; – Specifies the secondary DNS server’s IP address</li> <li>&lt;HOST-ALIAS-NAME1&gt; – Specifies a host alias, mapped to the secondary DNS server’s IP address. If the primary DNS server is unavailable, the secondary server is used.</li> </ul> <p><b>Note:</b> A network host alias maps a name to a single network host. For example, ‘alias host \$HOST 1.1.1.100’. In this example the host alias is ‘\$HOST’ and it maps to a single host ‘1.1.1.100’. For more information, see <a href="#">alias</a>.</p> |

### Examples

```

nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#dns-server 172.16.10.7
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#show context
 static-binding client-identifier test
 client-name RFID
 bootfile test.txt
 default-router 172.16.10.8 172.16.10.9
 dns-server 172.16.10.7
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#

```

### Related Commands

|           |                                                             |
|-----------|-------------------------------------------------------------|
| <b>no</b> | Resets values or disables DHCP pool static binding settings |
|-----------|-------------------------------------------------------------|

### domain-name (dhcpv4-pool-static-binding)

Sets the domain name for static binding configuration

Domain names are not case sensitive and contain alphabetic or numeric letters (or a hyphen). An FQDN consists of a host name plus a domain name. For example, computername.domain.com.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
domain-name <DOMAIN-NAME>
```

### Parameters

```
domain-name <DOMAIN-NAME>
```

|               |                                     |
|---------------|-------------------------------------|
| <DOMAIN-NAME> | Defines the DHCP pool’s domain name |
|---------------|-------------------------------------|

### Examples

```

nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#domain-name documentation
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#show context
 static-binding client-identifier test
 client-name RFID
 domain-name documentation
 bootfile test.txt

```

```

default-router 172.16.10.8 172.16.10.9
dns-server 172.16.10.7
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#

```

#### Related Commands

Resets values or disables the DHCP pool static binding settings

#### ip-address (dhcpv4-pool-static-binding)

Sets an IP address of the client using this host pool for DHCP resources

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
ip-address [<IP>|<HOST-ALIAS-NAME>]
```

#### Parameters

```
ip-address [<IP>|<HOST-ALIAS-NAME>]
```

|                                |                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;IP&gt;</b>              | Configures a fixed IP address (in dotted decimal format) of the client using this host pool                                                                                                                                                                                                                                                                              |
| <b>&lt;HOST-ALIAS-NAME&gt;</b> | Configures a host alias identifying the fixed IP address of the client using this host pool<br><br><b>Note:</b> A network host alias maps a name to a single network host. For example, 'alias host \$HOST 1.1.1.100'. In this example the host alias is '\$HOST' and it maps to a single host '1.1.1.100'. For more information, see <a href="#">alias</a> on page 237. |

#### Examples

```

nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#ip-address 172.16.10.9
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#show context
static-binding client-identifier test
ip-address 172.16.10.9
client-name RFID
domain-name documentation
bootfile test.txt
default-router 172.16.10.8 172.16.10.9
dns-server 172.16.10.7
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#

```

#### Related Commands

[no \(dhcpv4-pool-static-binding\)](#) on page 1467    Resets values or disables DHCP pool static binding settings

#### netbios-name-server (dhcpv4-pool-static-binding)

Configures the NetBIOS (WINS) name server's IP address. This server is used to resolve NetBIOS host names.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000

- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
netbios-name-server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

#### Parameters

```
netbios-name-server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

|                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>[&lt;IP&gt; &lt;HOST-ALIAS-NAME&gt;]</p>                                                                                                                                                                                                                      | <p>Configures the primary NetBIOS name server, using one of the following options:</p> <ul style="list-style-type: none"> <li>• &lt;IP&gt; – Specifies the primary NetBIOS name server’s IP address</li> <li>• &lt;HOST-ALIAS-NAME&gt; – Specifies a host alias, mapped to the primary NetBIOS name server’s IP address</li> </ul>                                                                                                     |
| <p>{&lt;IP1&gt; &lt;HOST-ALIAS-NAME1&gt;}</p>                                                                                                                                                                                                                    | <p>Optional. Configures the secondary NetBIOS name server, using one of the following options:</p> <ul style="list-style-type: none"> <li>• &lt;IP1&gt; – Specifies the secondary NetBIOS name server’s IP address</li> <li>• &lt;HOST-ALIAS-NAME1&gt; – Specifies a host alias, mapped to the secondary NetBIOS name server’s IP address. If the primary NetBIOS name server is unavailable, the secondary server is used.</li> </ul> |
| <p><b>Note:</b> A network host alias maps a name to a single network host. For example, ‘alias host \$HOST 1.1.1.100’. In this example the host alias is ‘\$HOST’ and it maps to a single host ‘1.1.1.100’. For more information, see <a href="#">alias</a>.</p> |                                                                                                                                                                                                                                                                                                                                                                                                                                        |

#### Examples

```
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#netbios-name-server
172.16.10.23
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#show context
static-binding client-identifier test
ip-address 172.16.10.9
client-name RFID
domain-name documentation
bootfile test.txt
default-router 172.16.10.8 172.16.10.9
dns-server 172.16.10.7
netbios-name-server 172.16.10.23
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#
```

#### Related Commands

|                                                                     |                                                                    |
|---------------------------------------------------------------------|--------------------------------------------------------------------|
| <p><a href="#">no (dhcpv4-pool-static-binding)</a> on page 1467</p> | <p>Resets values or disables DHCP pool static binding settings</p> |
|---------------------------------------------------------------------|--------------------------------------------------------------------|

#### netbios-node-type (dhcpv4-pool-static-binding)

Configures different predefined NetBIOS node types. The NetBIOS node defines the way a device resolves NetBIOS names to IP addresses.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
netbios-node-type [b-node|h-node|m-node|p-node]
```

#### Parameters

```
netbios-node-type [b-node|h-node|m-node|p-node]
```

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [b-node h-node m-node p-node] | <p>Defines the netbios node type</p> <ul style="list-style-type: none"> <li>• b-node – Sets the node type as broadcast. Uses broadcasts to query nodes on the network for the owner of a NetBIOS name.</li> <li>• h-node – Sets the node type as hybrid. Uses a combination of two or more nodes.</li> <li>• m-node – Sets the node type as mixed. A mixed node uses broadcasted queries to find a node, and failing that, queries a known p-node name server for the address.</li> <li>• p-node – Sets the node type as peer-to-peer. Uses directed calls to communicate with a known NetBIOS name server (such as a WINS server), for the IP address of a NetBIOS machine.</li> </ul> |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```

nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#netbios-node-type b-node
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#show context
static-binding client-identifier test
ip-address 172.16.10.9
client-name RFID
domain-name documentation
netbios-node-type b-node
bootfile test.txt
default-router 172.16.10.8 172.16.10.9
dns-server 172.16.10.7
netbios-name-server 172.16.10.23
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#

```

### Related Commands

|                                                           |                                                             |
|-----------------------------------------------------------|-------------------------------------------------------------|
| <code>no (dhcpv4-pool-static-binding)</code> on page 1467 | Resets values or disables DHCP pool static binding settings |
|-----------------------------------------------------------|-------------------------------------------------------------|

### next-server (dhcpv4-pool-static-binding)

Configures the next server utilized in the boot process

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
next-server [<IP> | <HOST-ALIAS-NAME>]
```

### Parameters

```
next-server [<IP> | <HOST-ALIAS-NAME>]
```

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IP>              | Configures the next server's (the first server in the boot process) IP address                                                                                                                                                                                                                                                                                                                                                                                                               |
| <HOST-ALIAS-NAME> | <p>Configures a host alias, mapped to the next server's IP address</p> <ul style="list-style-type: none"> <li>• &lt;HOST-ALIAS-NAME&gt; – Specify the host alias name. It should be existing and configured.</li> </ul> <p><b>Note:</b> A host alias maps a name to a single network host. For example, 'alias host \$HOST 1.1.1.100'. In this example the host alias is '\$HOST' and it maps to a single host '1.1.1.100'. For more information, see <a href="#">alias</a> on page 237.</p> |

## Examples

```
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#next-server 172.16.10.24
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#show context
static-binding client-identifier test
ip-address 172.16.10.9
client-name RFID
domain-name documentation
netbios-node-type b-node
bootfile test.txt
default-router 172.16.10.8 172.16.10.9
dns-server 172.16.10.7
netbios-name-server 172.16.10.23
next-server 172.16.10.24
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#
```

## Related Commands

|                                                           |                                                             |
|-----------------------------------------------------------|-------------------------------------------------------------|
| <code>no (dhcpv4-pool-static-binding)</code> on page 1467 | Resets values or disables DHCP pool static binding settings |
|-----------------------------------------------------------|-------------------------------------------------------------|

## option (dhcpv4-pool-static-binding)

Configures raw DHCP options. The DHCP option must be configured under the DHCP server policy. The options configured under the DHCP pool/DHCP server policy can also be used in static-bindings.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
option <OPTION-NAME> [<DHCP-OPTION-IP> | <DHCP-OPTION-ASCII>]
```

## Parameters

```
option <OPTION-NAME> [<DHCP-OPTION-IP> | <DHCP-OPTION-ASCII>]
```

|                     |                                     |
|---------------------|-------------------------------------|
| <OPTION-NAME>       | Sets the name of the DHCP option    |
| <DHCP-OPTION-IP>    | Sets DHCP option as an IP address   |
| <DHCP-OPTION-ASCII> | Sets DHCP option as an ASCII string |

## Usage Guidelines

Defines non standard DHCP option codes (0-254)



### Note

An option name in ASCII format accepts a backslash (\) as an input, but is not displayed in the output (Use show runnig config to view the output). Use a double backslash to represent a single backslash.

## Examples

```
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#option option1 172.16.10.10
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#show context
static-binding client-identifier test
client-name RFID
domain-name documentation
netbios-node-type b-node
netbios-name-server 172.16.10.23
```

```
next-server 172.16.10.24
option option1 172.16.10.10
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#
```

#### Related Commands

[no \(dhcpv4-pool-static-binding\)](#) on page 1467    Resets values or disables DHCP pool static binding settings

#### respond-via-unicast (dhcpv4-pool-static-binding)

Sends DHCP offer and acknowledgment as unicast messages

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
respond-via-unicast
```

#### Parameters

None

#### Examples

```
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#respond-via-unicast
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#show context
static-binding client-identifier test
client-name RFID
domain-name documentation
netbios-node-type b-node
netbios-name-server 172.16.10.23
next-server 172.16.10.24
option option1 172.16.10.10
respond-via-unicast
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#
```

#### Related Commands

[no \(dhcpv4-pool-static-binding\)](#) on page 1467    Resets values or disables DHCP pool static binding settings

#### static-route (dhcpv4-pool-static-binding)

Adds static routes to the static binding configuration. Use this option to add static routes installed on clients.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
static-route <IP/Mask> <Gateway-IP>
```

#### Parameters

```
static-route <IP/Mask> <Gateway-IP>
```

|              |                                                               |
|--------------|---------------------------------------------------------------|
| <IP/Mask>    | Specifies the IP destination prefix (for example, 10.0.0.0/8) |
| <Gateway-IP> | Specifies the gateway IP address                              |

### Examples

```

nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-1)#static-route 10.0.0.0/10
157.235.208.235
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#show context
static-binding client-identifier test
client-name RFID
domain-name documentation
netbios-node-type b-node
netbios-name-server 172.16.10.23
next-server 172.16.10.24
option option1 172.16.10.10
respond-via-unicast
static-route 10.0.0.0/10 157.235.208.235
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#

```

### Related Commands

|                                                              |                                                             |
|--------------------------------------------------------------|-------------------------------------------------------------|
| <a href="#">no (dhcpv4-pool-static-binding)</a> on page 1467 | Resets values or disables DHCP pool static binding settings |
|--------------------------------------------------------------|-------------------------------------------------------------|

## no (dhcpv4-pool-static-binding)

Negates or reverts static binding settings for the selected DHCP server policy

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```

no [bootfile|client-name|default-router|dns-server|domain-name|ip-address|
netbios-name-server|netbios-node-type|next-server|option|respond-via-unicast|
static-route]
no option <OPTION-NAME>
no option <OPTION-NAME>
no static-route <IP/MASK> <GATEWAY-IP>

```

### Parameters

no <PARAMETERS>

|                 |                                                                                |
|-----------------|--------------------------------------------------------------------------------|
| no <PARAMETERS> | Negates or reverts static binding settings for the selected DHCP server policy |
|-----------------|--------------------------------------------------------------------------------|

### Examples

The following example shows the DHCP pool settings before the 'no' commands are executed:

```

nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#show context
static-binding client-identifier test
ip-address 172.16.10.9
client-name RFID
domain-name documentation
netbios-node-type b-node
bootfile test.txt
default-router 172.16.10.8 172.16.10.9
dns-server 172.16.10.7
netbios-name-server 172.16.10.23

```

```

next-server 172.16.10.24
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#no bootfile
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#no ip-address
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#no default-router
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#no dns-server

```

The following example shows the DHCP pool settings after the 'no' commands are executed:

```

nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#show context
static-binding client-identifier test
client-name RFID
domain-name documentation
netbios-node-type b-node
netbios-name-server 172.16.10.23
next-server 172.16.10.24
nx9500-6C8809(config-dhcp-policy-test-pool-pool1-binding-test)#

```

### *ping (dhcpv4-server-policy-config)*

Configures the DHCP server's ping timeout interval. The controller uses the timeout to intermittently ping and discover whether a client requested IP address is available or in use.

#### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### **Syntax**

```
ping timeout <1-10>
```

#### **Parameters**

```
ping timeout <1-10>
```

|                |                                                                     |
|----------------|---------------------------------------------------------------------|
| timeout <1-10> | Sets the ping timeout from 1 - 10 seconds. The default is 1 second. |
|----------------|---------------------------------------------------------------------|

#### **Examples**

```

nx9500-6C8809(config-dhcp-policy-test)#ping timeout 2
nx9500-6C8809(config-dhcp-policy-test)#show context
dhcp-server-policy test
ping timeout 2
option option1 200 ascii
nx9500-6C8809(config-dhcp-policy-test)#

```

#### **Related Commands**

|                                                               |                                      |
|---------------------------------------------------------------|--------------------------------------|
| <a href="#">no (dhcpv4-server-policy-config)</a> on page 1471 | Resets the ping interval to 1 second |
|---------------------------------------------------------------|--------------------------------------|

### *option (dhcpv4-server-policy-config)*

Configures raw DHCP options. The DHCP option has to be configured in the DHCP server policy. The options configured in the DHCP pool/DHCP server policy can also be used in static bindings.



### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
option <OPTION-NAME> <0-250> [ascii|hexstring|ip]
```

### Parameters

```
option <OPTION-NAME> <0-250> [ascii|hexstring|ip]
```

|               |                                                    |
|---------------|----------------------------------------------------|
| <OPTION-NAME> | Configures the option name                         |
| <0-250>       | Configures the DHCP option code from 0 - 250       |
| ascii         | Configures the DHCP option as an ASCII string      |
| hexstring     | Configures the DHCP option as a hexadecimal string |
| ip            | Configures the DHCP option as an IP address        |

### Usage Guidelines

Defines non-standard DHCP option codes (0-254)



#### Note

An option name in ASCII format accepts a backslash (\) as an input, but is not displayed in the output. Use the **show > runnig > config** command to view the output. Use a double backslash to represent a single backslash.

### Examples

```
nx9500-6C8809(config-dhcp-policy-test)#option option1 200 ascii
nx9500-6C8809(config-dhcp-policy-test)#show context
dhcp-server-policy test
 option option1 200 ascii
nx9500-6C8809(config-dhcp-policy-test)#
```

### Related Commands

|                                                               |                             |
|---------------------------------------------------------------|-----------------------------|
| <a href="#">no (dhcpv4-server-policy-config)</a> on page 1471 | Removes DHCP server options |
|---------------------------------------------------------------|-----------------------------|

### *dhcp-server (dhcpv4-server-policy-config)*

Configures the activation-criteria (run-criteria) that triggers dynamic activation of DHCP service running on a redundancy device

In a managed wireless network, when the primary, active DHCP server fails (is unreachable), network clients are unable to access DHCP services, such as new IP address leasing and renewal of existing IP address leases. In such a scenario, the activation-criteria, when configured, triggers dynamic activation of the secondary DHCP server, allowing network clients to continue accessing DHCP services. The WiNG implementation provides activation-criteria options specific to a RF Domain, cluster setup, and a VRRP (Virtual Router Redundancy Protocol) master/client setup.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
dhcp-server activation-criteria [cluster-master|rf-domain-manager|vrrp-master]
```

### Parameters

```
dhcp-server activation-criteria [cluster-master|rf-domain-manager|vrrp-master]
```

|                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dhcp-server                                                        | Enables dynamic activation of the DHCP server, running on a redundancy device, based on the activation criteria specified                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| activation-criteria [cluster-master rf-domain-manager vrrp-master] | Configures the activation criteria. Specify one of the following options as the activation criteria: <ul style="list-style-type: none"><li>• cluster-master – Configures the cluster-master criteria in a cluster setup. Within a cluster, DHCP service is enabled on the cluster master. While it remains disabled on the other cluster members. In case of the cluster master failing, the cluster-master activation criteria, when configured, triggers dynamic activation of DHCP service on the new cluster master.</li><li>• rf-domain-manger – Configures the rf-domain-manager criteria on an RF Domain. Within a RF Domain, DHCP service is enabled on the RF Domain manager. While it remains disabled on the other devices within the RF Domain. In case of the RF Domain manager failing, the rf-domain-manager activation criteria, when configured, triggers dynamic activation of DHCP service on the new RF Domain manager.</li><li>• vrrp-master – Configures the vrrp-master criteria within a VRRP master/client setup. In such a setup, the DHCP service is enabled on the VRRP master. While it remains disabled on the other members. In case of the VRRP master failing, the vrrp-master activation criteria, when configured, triggers dynamic activation of DHCP service on the new VRRP master.</li></ul> |

### Examples

```
rfs4000-229D58(config-dhcp-policy-test)#dhcp-server activation-criteria rf-domain-manager
rfs4000-229D58(config-dhcp-policy-test)#show context
dhcp-server-policy test
dhcp-server activation-criteria rf-domain-manager
rfs4000-229D58(config-dhcp-policy-test)#
rfs4000-229D58(config-dhcp-policy-test)#no dhcp-server activation-criteria
rfs4000-229D58(config-dhcp-policy-test)#show context
dhcp-server-policy test
rfs4000-229D58(config-dhcp-policy-test)#
```

### Related Commands

|                                                               |                                                                                    |
|---------------------------------------------------------------|------------------------------------------------------------------------------------|
| <a href="#">no (dhcpv4-server-policy-config)</a> on page 1471 | Removes the DHCP service activation criteria configured on this DHCP server policy |
|---------------------------------------------------------------|------------------------------------------------------------------------------------|

## *no* (dhcpv4-server-policy-config)

Negates a command or sets its default. When used in the DHCP server configuration context, the 'no' command resets or reverts the DHCP server policy settings.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
no [bootp|dhcp-class|dhcp-pool|dhcp-server|option|ping]
no bootp ignore
no dhcp-class <DHCP-CLASS-NAME>
no dhcp-pool <DHCP-POOL-NAME>
no dhcp-server activation-criteria
no option <DHCP-OPTION>
no ping timeout
```

### Parameters

```
no <PARAMETERS>
```

```
no <PARAMETERS> Negates a command or sets its default. When used in the DHCP server configuration context, the 'no' command resets or reverts the DHCP server policy settings
```

### Examples

The following example shows the DHCP policy 'test' settings before the 'no' commands are executed:

```
nx9500-6C8809(config-dhcp-policy-test)#show context
dhcp-server-policy test
 bootp ignore
 dhcp-class dhcpclass1
 dhcp-pool pool1
 address 1.2.3.4 class dhcpclass1
 update dns override
 --More--
nx9500-6C8809(config-dhcp-policy-test)#
nx9500-6C8809(config-dhcp-policy-test)#no bootp ignore
nx9500-6C8809(config-dhcp-policy-test)#no dhcp-class dhcpclass1
nx9500-6C8809(config-dhcp-policy-test)#no dhcp-pool pool1
```

The following example shows the DHCP policy 'test' settings after the 'no' commands are executed:

```
nx9500-6C8809(config-dhcp-policy-test)#show context
dhcp-server-policy test
nx9500-6C8809(config-dhcp-policy-test)#
```

## dhcpv6-server-policy commands

DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes or other configuration attributes required on an IPv6 network.

DHCPv6 servers pass IPv6 network addresses to IPv6 clients. The DHCPv6 address assignment feature manages non duplicate addresses in the correct prefix based on the network where the host is connected. Assigned addresses can be from one or multiple pools. Additional options, such as the

default domain and DNS name-server address, can be passed back to the client. Address pools can be assigned for use on a specific interface or on multiple interfaces, or the server can automatically find the appropriate pool.

The following table summarizes the DHCPv6 server policy configuration mode commands:

**Table 45: DHCPv6-Server-Policy Config Mode Commands**

| Command                                                                         | Description                                                                                                   |
|---------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| <code>dhcpv6-pool (dhcpv6-server-policy-config)</code> on page 1472             | Creates a DHCPv6 pool and enters its configuration mode                                                       |
| <code>restrict-vendor-options (dhcpv6-server-policy-config)</code> on page 1480 | Configures this DHCPv6 server policy's DHCP option settings, such as enterprise (vendor ID)                   |
| <code>server-preference (dhcpv6-server-policy-config)</code> on page 1480       | Restricts the use of vendor-specific DHCP options on this DHCPv6 server policy                                |
| <code>option (dhcpv6-server-policy-config)</code> on page 1478                  | Configures this DHCP server's preference value. This value is sent in DHCP server replies to the IPv6 client. |
| <code>no (dhcpv6-server-policy-config)</code> on page 1481t                     | Negates or reverts this DHCPv6 server policy's settings                                                       |



**Note**

For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see **COMMON COMMANDS** on page 640.



**Note**

The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (\_) character. In other words, the name of a device cannot contain an underscore.

*dhcpv6-pool (dhcpv6-server-policy-config)*

Configures a DHCPv6 server address pool and enters its configuration mode

A DHCPv6 IPv6 pool is a resource from which IPv6 formatted addresses can be issued on DHCPv6 client requests. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.

**Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

**Syntax**

`dhcpv6-pool <DHCPv6-POOL-NAME>`

**Parameters**

`dhcpv6-pool <DHCPv6-POOL-NAME>`

|                                       |                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;DHCPv6-POOL-NAME&gt;</code> | <p>Creates a DHCPv6 server address pool</p> <ul style="list-style-type: none"> <li><code>&lt;POOL-NAME&gt;</code> - Specify a name that appropriately identifies this DHCPv6 address pool. If the pool does not exist, it is created. The pool name cannot be modified as part of the edit process. However, an obsolete address pool can be deleted.</li> </ul> |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```

nx9500-6C8809(config-dhcpv6-server-policy-test)#dhcpv6-pool DHCPv6Pool1
nx9500-6C8809(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#?
DHCPv6 pool Mode commands:
 dns-server DNS Servers
 domain-name Configure domain-name
 network Network on which DHCPv6 server will be deployed
 no Negate a command or set its defaults
 option Raw DHCPv6 options
 refresh-time Upper limit specifying the timer for which client should wait
 before refreshing information
 sip SIP server options

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#
nx9500-6C8809(config-dhcpv6-server-policy-test)#show context
dhcpv6-server-policy test
 dhcpv6-pool DHCPv6Pool1
 network 2002::/64
 domain-name TechPubs
 sip domain-name TechPubsSIP
 dns-server 2002::1
nx9500-6C8809(config-dhcpv6-server-policy-test)#

```

## Related Commands

The following table summarizes the DHCPv6 Pool configuration mode commands

|                                                             |                                                                                                                |
|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| <code>dns-server (dhcpv6-pool-config)</code> on page 1474   | Configures this DHCPv6 pool's DNS server                                                                       |
| <code>domain-name (dhcpv6-pool-config)</code> on page 1474  | Configures this DHCPv6 pool's domain name                                                                      |
| <code>network (dhcpv6-pool-config)</code> on page 1475      | Configures this DHCPv6 pool's network                                                                          |
| <code>option (dhcpv6-pool-config)</code> on page 1476       | Configures this DHCPv6 pool's raw DHCPv6 options. This is the vendor-specific option used in this DHCPv6 pool. |
| <code>refresh-time (dhcpv6-pool-config)</code> on page 1476 | Configures this DHCPv6 pool's refresh time in seconds                                                          |
| <code>sip (dhcpv6-pool-config)</code> on page 1477          | Configures this DHCPv6 pool's Session Initiation Protocol (SIP) server setting                                 |

`no (dhcpv6-pool-config)` on page 1478 Negates or reverts this DHCPv6 pool's settings

`no (dhcpv6-server-policy-config)` on page 1481 (dhcpv6-server-policy config) Removes this DHCPv6 pool

### dns-server (dhcpv6-pool-config)

Configures this DHCPv6 pool's DNS server. The DNS server supports all clients connected to networks supported by the DHCPv6 server.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
dns-server <IPv6> {<SECONDARY-IPv6>}
```

#### Parameters

```
dns-server <IPv6> {<SECONDARY-IPv6>}
```

|                  |                                                                                                                                                                                                                            |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IPv6>           | Configures the primary DNS server's IPv6 address <ul style="list-style-type: none"><li>• &lt;IPv6&gt; - Specify the DNS server's IPv6 address (the server associated with this DHCP pool).</li></ul>                       |
| <SECONDARY-IPv6> | Configures the secondary DNS server's IPv6 address <ul style="list-style-type: none"><li>• &lt;SECONDARY-IPv6&gt; - Specify the secondary DNS server's IPv6 address (the server associated with this DHCP pool).</li></ul> |

#### Examples

```
nx9500-6C8809(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#dns-server 2002::1
nx9500-6C8809(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#show context
dhcpv6-pool DHCPv6Pool1
 dns-server 2002::1
nx9500-6C8809(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#
```

#### Related Commands

`no (dhcpv6-pool-config)` on page 1478 Removes this DHCPv6 pool's configured DNS server settings

### domain-name (dhcpv6-pool-config)

Configures this DHCPv6 pool's domain name

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

domain-name <DOMAIN-NAME>

## Parameters

domain-name <DOMAIN-NAME>

|                           |                                                                        |
|---------------------------|------------------------------------------------------------------------|
| domain-name <DOMAIN-NAME> | Specify the DHCP pool's hostname or hostnames of the domain or domains |
|---------------------------|------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#domain-name TechPubs
nx9500-6C8809(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#show context
dhcpv6-pool DHCPv6Pool1
 domain-name TechPubs
 dns-server 2002::1
nx9500-6C8809(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#
```

## Related Commands

|                                      |                                        |
|--------------------------------------|----------------------------------------|
| no (dhcpv6-pool-config) on page 1478 | Removes this DHCPv6 pool's domain name |
|--------------------------------------|----------------------------------------|

## network (dhcpv6-pool-config)

Configures this DHCPv6 pool's network. Use this command to configure the address of the network on which this DHCP server is deployed.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

network [<IPv6/M> | <NETWORK-ALIAS-NAME> ]

## Parameters

network [<IPv6/M> | <NETWORK-ALIAS-NAME> ]

|                      |                                                                                     |
|----------------------|-------------------------------------------------------------------------------------|
| <IPv6/M>             | Specify this DHCPv6 pool network's IPv6 address and mask (for example, 1:2::1:0/96) |
| <NETWORK-ALIAS-NAME> | Specify this DHCPv6 pool network's alias name                                       |

## Examples

```
nx9500-6C8809(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#network 2002::0/64
nx9500-6C8809(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#show context
dhcpv6-pool DHCPv6Pool1
 network 2002::/64
 domain-name TechPubs
 dns-server 2002::1
nx9500-6C8809(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#
```

## Related Commands

|                                      |                                                                           |
|--------------------------------------|---------------------------------------------------------------------------|
| no (dhcpv6-pool-config) on page 1478 | Removes the network IPv6 address and mask configured for this DHCPv6 pool |
|--------------------------------------|---------------------------------------------------------------------------|

### option (dhcpv6-pool-config)

Configures this DHCPv6 pool's raw DHCPv6 options. This is the vendor-specific option used in this DHCPv6 pool.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
option <OPTION-NAME> [<DHCPv6-OPTION-IP> | <DHCPv6-OPTION-ASCII>]
```

Parameters

```
option <OPTION-NAME> [<DHCPv6-OPTION-IP> | <DHCPv6-OPTION-ASCII>]
```

|                       |                                       |
|-----------------------|---------------------------------------|
| <OPTION-NAME>         | Sets the name of the DHCPv6 option    |
| <DHCPv6-OPTION-IP>    | Sets DHCPv6 option as an IPv6 address |
| <DHCPv6-OPTION-ASCII> | Sets DHCPv6 option as an ASCII string |

Usage Guidelines

An option name in ASCII format accepts backslash (\) as an input but is not displayed in the output. Use the **show > running > config** command to view the output. Use a double backslash to represent a single backslash.

Examples

```
nx9500-6C8809(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#option DHCPv6Pool1Option
60
nx9500-6C8809(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#show context
dhcpv6-pool DHCPv6Pool1
network 2002::/64
domain-name TechPubs
dns-server 2002::1
option DHCPv6Pool1Option 60
nx9500-6C8809(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#
```

Related Commands

|                                                      |                                                 |
|------------------------------------------------------|-------------------------------------------------|
| <a href="#">no (dhcpv6-pool-config)</a> on page 1478 | Removes this DHCPv6 pool's DHCP option settings |
|------------------------------------------------------|-------------------------------------------------|

### refresh-time (dhcpv6-pool-config)

Configures this DHCPv6 pool's refresh time in seconds. This is the interval between two successive DHCP pool refreshes. The DHCP refresh process refreshes IPv6 client information.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000



## Syntax

```
refresh-time <600-4294967295>
```

## Parameters

```
refresh-time <600-4294967295>
```

|                                                                                                     |
|-----------------------------------------------------------------------------------------------------|
| refresh-time <600-4294967295> Specify this DHCPv6 pool's refresh time from 600 -4294967295 seconds. |
|-----------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#refresh-time 1000
nx9500-6C8809(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#show context
dhcpv6-pool DHCPv6Pool1
 network 2002::/64
 refresh-time 1000
 domain-name TechPubs
 dns-server 2002::1
 option DHCPv6Pool1Option 60
nx9500-6C8809(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#
```

## Related Commands

|                                                                                                                   |
|-------------------------------------------------------------------------------------------------------------------|
| <a href="#">no (dhcpv6-pool-config)</a> on page 1478 Removes or reverts the configured DHCPv6 pool's refresh time |
|-------------------------------------------------------------------------------------------------------------------|

## sip (dhcpv6-pool-config)

Configures this DHCPv6 pool's SIP (Session Initiation Protocol) server setting

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
sip [address <IPv6>|domain-name <DOMAIN-NAME>]
```

## Parameters

```
sip [address <IPv6>|domain-name <DOMAIN-NAME>]
```

|                                                                                                                                       |
|---------------------------------------------------------------------------------------------------------------------------------------|
| sip [address <IPv6> domain-name <DOMAIN-NAME>] Configures the SIP server's setting, such as address and/or domain name <DOMAIN-NAME>] |
|---------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#sip domain-name
TechPubsSIP
nx9500-6C8809(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#show context
dhcpv6-pool DHCPv6Pool1
 network 2002::/64
 refresh-time 1000
 domain-name TechPubs
 sip domain-name TechPubsSIP
 dns-server 2002::1
 option DHCPv6Pool1Option 60
nx9500-6C8809(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#
```

## Related Commands

|                                                   |                                               |
|---------------------------------------------------|-----------------------------------------------|
| <code>no (dhcpv6-pool-config)</code> on page 1478 | Removes this DHCPv6 pool's SIP server setting |
|---------------------------------------------------|-----------------------------------------------|

## **no (dhcpv6-pool-config)**

Negates a command or sets its default. When used in the DHCPv6 pool configuration context, the 'no' command resets or reverts the DHCPv6 pool's settings.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
no [dns-server | domain-name | network | option | refresh-time | sip]
```

### Parameters

```
no <PARAMETERS>
```

|                                    |                                                                                                                                                           |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>no &lt;PARAMETERS&gt;</code> | Negates a command or sets its default. When used in the DHCPv6 pool configuration context, the 'no' command resets or reverts the DHCPv6 pool's settings. |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#show context
dhcpv6-pool DHCPv6Pool1
 network 2002::/64
 refresh-time 1000
 domain-name TechPubs
 sip domain-name TechPubsSIP
 dns-server 2002::1
 option DHCPv6Pool1Option 60
nx9500-6C8809(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#
nx9500-6C8809(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#no option
DHCPv6Pool1Option
nx9500-6C8809(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#no refresh-time
nx9500-6C8809(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#show context
dhcpv6-pool DHCPv6Pool1
 network 2002::/64
 domain-name TechPubs
 sip domain-name TechPubsSIP
 dns-server 2002::1
nx9500-6C8809(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#
```

## *option (dhcpv6-server-policy-config)*

Configures this DHCPv6 server policy's DHCP option settings, such enterprise (vendor) ID

DHCPv6 services are available for specific IP interfaces. A pool (or range) of IPv6 network addresses and DHCPv6 options can be created for each IPv6 interface defined. This range of addresses can be made available to DHCPv6 enabled devices on either a permanent or leased basis. DHCPv6 options are provided to each client with a DHCPv6 response and provide DHCPv6 clients information required to access network resources (default gateway, domain name, DNS server and WINS server configuration). An option exists to identify the vendor and functionality of a DHCPv6 client. The information is a

variable-length string of characters (or octets) with a meaning specified by the vendor of the DHCPv6 client.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
option <OPTION-NAME> <0-254> [ascii|hexstring|ipv6] <1-4294967295>
```

### Parameters

```
option <OPTION-NAME> <0-254> [ascii|hexstring|ipv6] <1-4294967295>
```

|                      |                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| option <OPTION-NAME> | Specify a unique name for this DHCP option. The name should describe option's function.                                                                                                                                                                                                                                                                                                  |
| <0-254>              | Specify a DHCP option code for this option. <ul style="list-style-type: none"> <li>• &lt;0-254&gt; - Specify a value from 0 -254.</li> </ul> <p>The system allows only one code, of the same value, for each DHCP option used in each DHCPv6 server policy.</p>                                                                                                                          |
| ascii                | Specifies the option type as ASCII (sends an ASCII compliant string to the client)                                                                                                                                                                                                                                                                                                       |
| hexstring            | Specifies the option type as a string of hexadecimal characters (sends a hexadecimal string to the client)                                                                                                                                                                                                                                                                               |
| ipv6                 | Specifies the option type as IPv6 address (sends an IPv6 compatible address to the client)                                                                                                                                                                                                                                                                                               |
| <1-4294967295>       | This parameter is common to all option types. <ul style="list-style-type: none"> <li>• &lt;1-4294967295&gt; - Specifies the enterprise (vendor) ID. Specify a value from 1 - 4294967295. The option code (1) is reserved for subnet-mask and cannot be used.</li> </ul> <p>Each vendor should have a unique vendor ID used by the DHCP server to issue vendor-specific DHCP options.</p> |

### Examples

```
nx9500-6C8809(config-dhcpv6-server-policy-test)#option DHCPServerOption1 10 ascii 50
nx9500-6C8809(config-dhcpv6-server-policy-test)#show context
dhcpv6-server-policy test
 option DHCPServerOption1 10 ascii 50
 dhcpv6-pool DHCPv6Pool1
 network 2002::/64
 domain-name TechPubs
 sip domain-name TechPubsSIP
 dns-server 2002::1
nx9500-6C8809(config-dhcpv6-server-policy-test)#
```

### Related Commands

|                                                      |                                                                                    |
|------------------------------------------------------|------------------------------------------------------------------------------------|
| <b>no (dhcpv6-server-policy-config)</b> on page 1481 | Removes the DHCPv6 server option settings configured for this DHCPv6 server policy |
|------------------------------------------------------|------------------------------------------------------------------------------------|

### *restrict-vendor-options (dhcpv6-server-policy-config)*

Restricts the use of vendor-specific DHCP options on this DHCPv6 server policy. When restricted, vendor-specific DHCP options, configured on this DHCPv6 server policy, are not included in the DHCPv6 server replies to IPv6 clients.

#### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### **Syntax**

```
restrict-vendor-options
```

#### **Parameters**

None

#### **Examples**

```
nx9500-6C8809(config-dhcpv6-server-policy-test)#restrict-vendor-options
nx9500-6C8809(config-dhcpv6-server-policy-test)#show context
dhcpv6-server-policy test
 option DHCPv6ServerOption1 10 ascii 50
 dhcpv6-pool DHCPv6Pool1
 network 2002::/64
 domain-name TechPubs
 sip domain-name TechPubsSIP
 dns-server 2002::1
 restrict-vendor-options
nx9500-6C8809(config-dhcpv6-server-policy-test)#
```

#### **Related Commands**

|                                                            |                                                                                                    |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| <code>no (dhcpv6-server-policy-config)</code> on page 1481 | Removes restriction on sending of vendor-specific options in DHCPv6 server replies to IPv6 clients |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------------|

### *server-preference (dhcpv6-server-policy-config)*

Configures this DHCPv6 server's preference value. When configured, the server preference value is included in the DHCPv6 server's replies to IPv6 clients.

#### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### **Syntax**

```
server-preference <0-255>
```

## Parameters

server-preference <0-255>one

|                           |                                                                                                 |
|---------------------------|-------------------------------------------------------------------------------------------------|
| server-preference <0-255> | Configures this DHCP server's preference value                                                  |
|                           | <ul style="list-style-type: none"><li>• &lt;0-255&gt; - Specify a value from 0 - 255.</li></ul> |

## Examples

```
nx9500-6C8809(config-dhcpv6-server-policy-test)#server-preference 1
nx9500-6C8809(config-dhcpv6-server-policy-test)#show context
dhcpv6-server-policy test
 option DHCPServerOption1 10 ascii 50
 dhcpv6-pool DHCPv6Pool1
 network 2002::/64
 domain-name TechPubs
 sip domain-name TechPubsSIP
 dns-server 2002::1
 server-preference 1
 restrict-vendor-options
nx9500-6C8809(config-dhcpv6-server-policy-test)#
```

## Related Commands

|                                                               |                                               |
|---------------------------------------------------------------|-----------------------------------------------|
| <a href="#">no (dhcpv6-server-policy-config) on page 1481</a> | Removes this DHCPv6 server's preference value |
|---------------------------------------------------------------|-----------------------------------------------|

*no (dhcpv6-server-policy-config)*

Negates or reverts this DHCPv6 server policy's settings

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

no [dhcpv6-pool|option|restrict-vendor-options|server-preference]

## Parameters

no <PARAMETERS>

|                 |                                                       |
|-----------------|-------------------------------------------------------|
| no <PARAMETERS> | Negates or reverts this DHCPv6 server policy settings |
|-----------------|-------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-dhcpv6-server-policy-test)#show context
dhcpv6-server-policy test
 option DHCPServerOption1 10 ascii 50
 dhcpv6-pool DHCPv6Pool1
 network 2002::/64
 domain-name TechPubs
 sip domain-name TechPubsSIP
 dns-server 2002::1
 server-preference 1
```

---

```
restrict-vendor-options
nx9500-6C8809(config-dhcpv6-server-policy-test)#
nx9500-6C8809(config-dhcpv6-server-policy-test)#no restrict-vendor-options
nx9500-6C8809(config-dhcpv6-server-policy-test)#no server-preference
nx9500-6C8809(config-dhcpv6-server-policy-test)#show context
dhcpv6-server-policy test
 option DHCPServerOption1 10 ascii 50
 dhcpv6-pool DHCPv6Pool1
 network 2002::/64
 domain-name TechPubs
 sip domain-name TechPubsSIP
 dns-server 2002::1
nx9500-6C8809(config-dhcpv6-server-policy-test)#
```

# FIREWALL POLICY

## FIREWALL-POLICY

---

This chapter summarizes the firewall policy commands in the CLI command structure.

A firewall protects a network from attacks and unauthorized access from outside the network. Simultaneously, it allows authorized users to access required resources. Firewalls work on multiple levels. Some work at layers 1, 2 and 3 to inspect each packet. The packet is either passed, dropped or rejected based on rules configured on the firewall.

Firewalls use application layer filtering to enforce compliance. These firewalls can understand applications and protocols and can detect if an unauthorized protocol is being used, or an authorized protocol is being abused in any malicious way.

The third set of firewalls, 'Stateful Firewalls', consider the placement of individual packets within each packet in the series of packets being transmitted. If there is a packet that does not fit into the sequence, it is automatically identified and dropped.

Use (config) instance to configure firewall policy commands. To navigate to the *config-fw-policy* instance, use the following commands:

```
<DEVICE>(config)#firewall-policy <POLICY-NAME>
nx9500-6C8809(config)#firewall-policy test
nx9500-6C8809(config-fw-policy-test)#?
Firewall policy Mode commands:
 acl-logging Log on flow creating traffic
 alg Enable ALG
 clamp Clamp value
 dhcp-offer-convert Enable conversion of broadcast dhcp offers to
 unicast
 dns-snoop DNS Snooping
 firewall Configure global firewall
 flow Firewall flow
 ip Internet Protocol (IP)
 ip-mac Action based on ip-mac table
 ipv6 Internet Protocol version 6 (IPv6)
 ipv6-mac Action based on ipv6-mac table
 logging Firewall enhanced logging
 no Negate a command or set its defaults
 proxy-arp Enable generation of ARP responses on behalf
 of another device
 proxy-nd Enable generation of ND responses (for IPv6)
 on behalf of another device
 stateful-packet-inspection-l2 Enable stateful packet inspection in layer2
 firewall
 storm-control Storm-control
 virtual-defragmentation Enable virtual defragmentation for IPv4 and
 IPv6 packets (recommended for proper
 functioning of firewall)

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
```

```

help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or
 terminal

```

```
nx9500-6C8809(config-fw-policy-test)#
```

## firewall-policy-commands

The following table summarizes the default firewall policy configuration commands:

*Table: Firewall-Policy Config Mode Commands*

| Command                                                    | Description                                                                   |
|------------------------------------------------------------|-------------------------------------------------------------------------------|
| <a href="#">acl-logging</a> on page 1485                   | Enables logging on flow creating traffic                                      |
| <a href="#">alg</a> on page 1485                           | Enables an algorithm                                                          |
| <a href="#">clamp</a> on page 1486                         | Sets a clamp value to limit TCP MSS to inner path-MTU for tunneled packets    |
| <a href="#">dhcp-offer-convert</a> on page 1487            | Enables the conversion of broadcast DHCP offers to unicast                    |
| <a href="#">dns-snoop</a> on page 1488                     | Sets the timeout value for DNS entries                                        |
| <a href="#">firewall</a> on page 1488                      | Configures the wireless firewall                                              |
| <a href="#">flow</a> on page 1489                          | Defines a session flow timeout                                                |
| <a href="#">ip</a> on page 1490                            | Configures IP components on this firewall policy                              |
| <a href="#">ip-mac</a> on page 1497                        | Defines an action based on IP-MAC table                                       |
| <a href="#">ipv6</a> on page 1499                          | Configures IPv6 components on this firewall policy                            |
| <a href="#">ipv6-mac</a> on page 1502                      | Defines an action based on IPv6-MAC table                                     |
| <a href="#">logging</a> on page 1504                       | Enables enhanced firewall logging                                             |
| <a href="#">proxy-arp</a> on page 1506                     | Enables the generation of ARP responses on behalf of another device           |
| <a href="#">proxy-nd</a> on page 1506                      | Enables the generation of ND responses (for IPv6) on behalf of another device |
| <a href="#">stateful-packet-inspection-12</a> on page 1507 | Enables stateful packets-inspection in layer 2 firewall                       |
| <a href="#">storm-control</a> on page 1507                 | Defines storm control and logging settings                                    |
| <a href="#">virtual-defragmentation</a> on page 1509       | Enables virtual defragmentation of IPv4 packets                               |
| <a href="#">no</a> on page 1510                            | Negates a command or reverts settings to their default                        |



### Note

For more information on common commands (clrsr, commit, help, revert, service, show, write, and exit), see [COMMON COMMANDS](#) on page 640.





#### Note

The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore ( `_` ) character. In other words, the name of a device cannot contain an underscore.

### *acl-logging*

Enables logging on flow creating traffic

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
acl-logging
```

#### Parameters

None

#### Examples

```
nx9500-6C8809(config-fw-policy-testFW)#acl-logging
nx9500-6C8809(config-fw-policy-testFW)#show context include-factory | include acl-logging
 acl-logging
nx9500-6C8809(config-fw-policy-testFW)#
```

#### Related Commands

|                                                                           |
|---------------------------------------------------------------------------|
| <a href="#">no</a> on page 1510 Disables logging on flow creating traffic |
|---------------------------------------------------------------------------|

### *alg*

Enables traffic filtering at the application layer using the ALG (Application Layer Gateway) feature

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
alg [dns|facetime|ftp|pptp|sccp|sip|tftp]
```

#### Parameters

```
alg [dns|facetime|ftp|pptp|sccp|sip|tftp]
```

|          |                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| alg      | Enables traffic filtering at the application layer. The ALG provides filters for the following common protocols: <b>DNS, Facetime, FTP, PPTP, SCCP, SIP,</b> and <b>TFTP</b> .                                                                                                                                                                                                                      |
| dns      | Allows DNS (Domain Name System) traffic through the firewall using its default ports. This option is enabled by default. When enabled, you can easily permit or deny traffic based on a packet's DNS name, instead of the IP address. Use this option when configuring ACLs allowing or denying traffic for Web sites that have a single domain name resolving to any one of multiple IP addresses. |
| facetime | Allows Apple's FaceTime video calling traffic through the firewall using its default ports. This option is disabled by default.                                                                                                                                                                                                                                                                     |
| ftp      | Allows FTP (File Transfer Protocol) traffic through the firewall using its default ports. This option is enabled by default.                                                                                                                                                                                                                                                                        |
| pptp     | Allows PPTP (Point-to-Point Tunneling Protocol) traffic through the firewall using its default ports. PPTP, a network protocol, enables secure transfer of data from a remote client to an enterprise server by encapsulating PPP packets into IP datagrams for transmission over the Internet or other public TCP/IP-based networks. This option is enabled by default.                            |
| sccp     | Allows SCCP (Signalling Connection Control Part) traffic through the firewall using its default ports. This option is disabled by default. SCCP is a network protocol that provides routing, flow control and error correction in telecommunication networks.                                                                                                                                       |
| sip      | Allows SIP (Session Initiation Protocol) traffic through the firewall using its default ports. This option is disabled by default.                                                                                                                                                                                                                                                                  |
| tftp     | Enables the TFTP (Trivial File Transfer Protocol) algorithm. When enabled, allows TFTP traffic through the firewall using its default ports. This option is enabled by default.                                                                                                                                                                                                                     |

### Examples

```

nx9500-6C8809(config-fw-policy-testFW)#show context
nx9500-6C8809(config-fw-policy-testFW)#show context
firewall-policy testFW
 no ip dos tcp-sequence-past-window
 alg facetime
nx9500-6C8809(config-fw-policy-testFW)#

```

### Related Commands

|                        |                                         |
|------------------------|-----------------------------------------|
| <b>no</b> on page 1510 | Removes or reverts ALG related settings |
|------------------------|-----------------------------------------|

### *clamp*

This option limits the TCP MSS (Maximum Segment Size) to the size of the MTU (Maximum Transmission Unit) discovered by path MTU discovery for the inner protocol. This ensures the packet traverses through the inner protocol without fragmentation. This option is enabled by default.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
clamp tcp-mss
```

## Parameters

```
clamp tcp-mss
```

|         |                                                                                     |
|---------|-------------------------------------------------------------------------------------|
| tcp-mss | Limits the TCP MSS size to the MTU value of the inner protocol for tunneled packets |
|---------|-------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-fw-policy-test)#clamp tcp-mss
nx9500-6C8809(config-fw-policy-testFW)#show context include-factory | include clamp
clamp tcp-mss
nx9500-6C8809(config-fw-policy-testFW)#
```

## Related Commands

|                              |                                  |
|------------------------------|----------------------------------|
| <code>no</code> on page 1510 | Disables limiting of the TCP MSS |
|------------------------------|----------------------------------|

## *dhcp-offer-convert*

Enables the conversion of broadcast DHCP offers to unicast. Converting DHCP broadcast traffic to unicast traffic can help reduce network traffic loads. This option is disabled by default.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
dhcp-offer-convert
```

## Parameters

None

## Examples

```
nx9500-6C8809(config-fw-policy-testFW)#dhcp-offer-convert
nx9500-6C8809(config-fw-policy-testFW)#show context
firewall-policy testFW
no ip dos tcp-sequence-past-window
dhcp-offer-convert
alg facetime
nx9500-6C8809(config-fw-policy-testFW)#
```

## Related Commands

|                              |                                                             |
|------------------------------|-------------------------------------------------------------|
| <code>no</code> on page 1510 | Disables the conversion of broadcast DHCP offers to unicast |
|------------------------------|-------------------------------------------------------------|

## *dns-snoop*

Sets the timeout interval for DNS snoop table entries. DNS snoop entries provide information, such as client to IP address and client to default gateway(s) mappings. This information is used to detect if the client is sending routed packets to a wrong MAC address.

### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### **Syntax**

```
dns-snoop entry-timeout <30-86400>
```

### **Parameters**

```
dns-snoop entry-timeout <30-86400>
```

|                             |                                                                                                                                                                                                                            |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| entry-timeout<br><30-86400> | Sets the DNS snoop table entry timeout interval from 30 - 86400 seconds. An entry is retained in the DNS snoop table only for the specified time, and is deleted once this time is exceeded. The default is 1,800 seconds. |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### **Examples**

```
nx9500-6C8809(config-fw-policy-testFW)#dns-snoop entry-timeout 1200
nx9500-6C8809(config-fw-policy-testFW)#show context
firewall-policy testFW
 no ip dos tcp-sequence-past-window
 dhcp-offer-convert
 alg facetime
 dns-snoop entry-timeout 1200
nx9500-6C8809(config-fw-policy-testFW)#
```

### **Related Commands**

|                              |                                                    |
|------------------------------|----------------------------------------------------|
| <code>no on page 1510</code> | Removes the DNS snoop table entry timeout interval |
|------------------------------|----------------------------------------------------|

## *firewall*

Enables the firewall. The Firewall is enabled by default.

### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### **Syntax**

```
firewall enable
```

## Parameters

firewall enable

|                 |                           |
|-----------------|---------------------------|
| firewall enable | Enables wireless firewall |
|-----------------|---------------------------|

## Examples

```
nx9500-6C8809(config-fw-policy-testFW)#firewall enable
nx9500-6C8809(config-fw-policy-testFW)#show context include-factory | include firewall
firewall-policy testFW
 firewall enable
 ipv6 firewall enable
nx9500-6C8809(config-fw-policy-testFW)#
```

## Related Commands

|                 |                       |
|-----------------|-----------------------|
| no on page 1510 | Disables the firewall |
|-----------------|-----------------------|

## flow

Defines the session flow timeout interval for different packet types

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
flow [dhcp|timeout]
flow dhcp stateful
flow timeout [icmp|other|tcp|udp]
flow timeout [icmp|other] <1-32400>
flow timeout udp <15-32400>
flow timeout tcp [close-wait|reset|setup|stateless-fin-or-reset| stateless-general]
<1-32400>
flow timeout tcp established <15-32400>
```

## Parameters

flow dhcp stateful

|          |                                                                                |
|----------|--------------------------------------------------------------------------------|
| dhcp     | Configures DHCP packet flow                                                    |
| stateful | Performs a stateful check on DHCP packets. This feature is enabled by default. |

flow timeout [icmp|other] <1-32400>

|           |                                                                                             |
|-----------|---------------------------------------------------------------------------------------------|
| timeout   | Configures a packet timeout                                                                 |
| icmp      | Configures the timeout for ICMP packets. The default is 30 seconds.                         |
| other     | Configures the timeout for packets other than ICMP, TCP, or UDP. The default is 30 seconds. |
| <1-32400> | Specify the timeout from 1 - 32400 seconds.                                                 |

flow timeout udp <15-32400>

|            |                                                                    |
|------------|--------------------------------------------------------------------|
| timeout    | Configures a packet timeout                                        |
| udp        | Configures the timeout for UDP packets. The default is 30 seconds. |
| <15-32400> | Specify the timeout from 15 - 32400 seconds.                       |

```
flow timeout tcp [close-wait|reset|setup|stateless-fin-or-reset|stateless-general]
<1-32400>
```

|                        |                                                                                                         |
|------------------------|---------------------------------------------------------------------------------------------------------|
| timeout                | Configures a packet timeout                                                                             |
| tcp                    | Configures the timeout for TCP packets                                                                  |
| close-wait             | Configures the closed TCP flow timeout. The default is 10 seconds.                                      |
| reset                  | Configures the reset TCP flow timeout. The default is 10 seconds.                                       |
| setup                  | Configures the opening TCP flow timeout. The default is 10 seconds.                                     |
| stateless-fin-or-reset | Configures stateless TCP flow timeout created with the FIN or RESET packets. The default is 10 seconds. |
| stateless-general      | Configures the stateless TCP flow timeout. The default is 90 seconds (1 m 30s).                         |
| <1-32400>              | Specify the timeout from 1 - 32400 seconds.                                                             |

```
flow timeout tcp established <15-32400>
```

|             |                                                                           |
|-------------|---------------------------------------------------------------------------|
| timeout     | Configures the packet timeout                                             |
| tcp         | Configures the timeout for TCP packets                                    |
| established | Configures the established TCP flow timeout. The default is 5400 seconds. |
| <15-32400>  | Specify the timeout from 15 - 32400 seconds.                              |

## Examples

```
nx9500-6C8809(config-fw-policy-testFW)#flow timeout udp 10000
nx9500-6C8809(config-fw-policy-testFW)#flow timeout icmp 16000
nx9500-6C8809(config-fw-policy-testFW)#flow timeout other 16000
nx9500-6C8809(config-fw-policy-testFW)#flow timeout tcp established 1500
nx9500-6C8809(config-fw-policy-testFW)#show context
firewall-policy testFW
no ip dos tcp-sequence-past-window
flow timeout icmp 16000
flow timeout udp 10000
flow timeout tcp established 1500
flow timeout other 16000
dhcp-offer-convert
alg facetime
dns-snoop entry-timeout 1200
nx9500-6C8809(config-fw-policy-testFW)#
```

## Related Commands

|                 |                                                                         |
|-----------------|-------------------------------------------------------------------------|
| no on page 1510 | Removes session timeout intervals configured for different packet types |
|-----------------|-------------------------------------------------------------------------|

*ip*

Configures IP components

## Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
ip [dos|tcp]
ip dos {ascend|broadcast-multicast-icmp|chargen|fraggle|ftp-bounce|invalid-protocol|
ip-ttl-zero|ipsproof|land|option-route|router-advt|router-solicit|smurf|snork|tcp-bad-
sequence|
tcp-fin-scan|tcp-intercept|tcp-max-incomplete|tcp-null-scan|tcp-post-syn|tcp-sequence-past-
window|
tcp-xmas-scan|tcphdrfrag|twinge|udp-short-hdr|winnuke}
ip dos {ascend|broadcast-multicast-icmp|chargen|fraggle|ftp-bounce|invalid-protocol|
ip-ttl-zero|ipsproof|land|option-route|router-advt|router-solicit|smurf|snork|tcp-bad-
sequence|
tcp-fin-scan|tcp-intercept|tcp-null-scan|tcp-post-scan|tcp-sequence-past-window|tcp-xmas-
scan|
tcphdrfrag|twinge|udp-short-hdr|winnuke} [log-and-drop|log-only] log-level [<0-7>|alerts|
critical|
debugging|emergencies|errors|informational|notifications|warnings]
ip dos {ascend|broadcast-multicast-icmp|chargen|fraggle|ftp-bounce|invalid-protocol|
ip-ttl-zero|ipsproof|land|option-route|router-advt|router-solicit|smurf|snork|tcp-bad-
sequence|
tcp-fin-scan|tcp-intercept|tcp-null-scan|tcp-post-scan|tcp-sequence-past-window|tcp-xmas-
scan|
tcphdrfrag|twinge|udp-short-hdr|winnuke} [drop-only]
ip dos tcp-max-incomplete [high|low] <1-1000>
ip tcp [adjust-mss|optimize-unnecessary-resends|recreate-flow-on-out-of-state-syn|
validate-icmp-unreachable|validate-rst-ack-number|validate-rst-seq-number]
ip tcp adjust-mss <472-1460>
ip tcp [optimize-unnecessary-resends|recreate-flow-on-out-of-state-syn|validate-icmp-
unreachable|
validate-rst-ack-number|validate-rst-seq-number]
```

## Parameters

```
ip dos {ascend|broadcast-multicast-icmp|chargen|fraggle|ftp-bounce|invalid-protocol|
ip-ttl-zero|ipsproof|land|option-route|router-advt|router-solicit|smurf|snork|tcp-bad-
sequence|
tcp-fin-scan|tcp-intercept|tcp-null-scan|tcp-post-scan|tcp-sequence-past-window|tcp-xmas-
scan|
tcphdrfrag|twinge|udp-short-hdr|winnuke} [log-and-drop|log-only]
log-level [<0-7>|alerts|critical|debug|emergencies|errors|informational|notifications|
warnings]
```

|                          |                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dos                      | Identifies IP events as DoS events                                                                                                                                                                                                                                                                                                              |
| ascend                   | Optional. Detects ASCEND DoS attacks<br>Ascend DoS attacks target known vulnerabilities in various versions of Ascend routers. Ascend routers listen on UDP port 9 for packets from Ascend's Java Configurator. Sending a formatted packet to this port can cause an Ascend router to crash.                                                    |
| broadcast-multicast-icmp | Optional. Detects broadcast or multicast ICMP Dos attacks<br>Broadcast or multicast ICMP DoS attacks take advantage of ICMP behavior in response to echo replies. These attacks spoof the source address of the target and send ICMP broadcast or multicast echo requests to the rest of the network, flooding the target machine with replies. |

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| chargen          | <p>Optional. Detects Chargen attacks</p> <p>The chargen (Character Generation Protocol) is an IP suite service primarily used for testing and debugging networks. It is also used as a source of generic payload for bandwidth and QoS measurements.</p> <p>The Chargen attack establishes a Telnet connection to port 19 and attempts to use the character generator service to create a string of characters which is then directed to the DNS service on port 53 to disrupt DNS services.</p>                                                                                                                                                                                                                            |
| fraggle          | <p>Optional. Detects Fraggle DoS attacks</p> <p>The Fraggle DoS attack uses a list of broadcast addresses to send spoofed UDP packets to each broadcast address' echo port (port 7). Each of those addresses that have port 7 open will respond to the request generating a lot of traffic on the network. For those that do not have port 7 open they will send an unreachable message back to the originator, further clogging the network with more traffic.</p>                                                                                                                                                                                                                                                         |
| ftp-bounce       | <p>Optional. Detects FTP bounce attacks</p> <p>A FTP bounce attack is a MIM attack that enables an attacker to open a port on a different machine using FTP. FTP requires that when a connection is requested by a client on the FTP port (21), another connection must open between the server and the client. To confirm, the PORT command has the client specify an arbitrary destination machine and port for the data connection. This is exploited by the attacker to gain access to a device that may not be the originating client.</p>                                                                                                                                                                             |
| invalid-protocol | <p>Optional. Enables a check for an invalid protocol number</p> <p>Attackers may use vulnerability in the endpoint implementation by sending invalid protocol fields, or may misuse the misinterpretation of endpoint software. This can lead to inadvertent leakage of sensitive network topology information, call hijacking, or a DoS attack.</p>                                                                                                                                                                                                                                                                                                                                                                        |
| ip-ttl-zero      | <p>Optional. Enables a check for the TCP/IP TTL field having a value of zero (0)</p> <p>The TCP IP TTL Zero DoS attack sends spoofed multicast packets onto the network which have a TTL (Time to Live) of 0. This causes packets to loop back to the spoofed originating machine, and can cause the network to overload.</p>                                                                                                                                                                                                                                                                                                                                                                                               |
| ipsproof         | <p>Optional. Enables a check for the IP spoofing DoS attack</p> <p>IP Spoof is a category of DoS attack that sends IP packets with forged source addresses. This can hide the identity of the attacker.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| land             | <p>Optional. Detects LAND DoS attacks</p> <p>A LAND (Local Area Network Denial) is a DoS attack where IP packets are spoofed and sent to a device where the source IP and destination IP of the packet are the target device's IP, and similarly, the source port and destination port are open ports on the same device. This causes the attacked device to reply to itself continuously.</p>                                                                                                                                                                                                                                                                                                                              |
| option-route     | <p>Optional. Enables an IP Option Record Route DoS check</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| router-adv       | <p>Optional. Detects router-advertisement attacks</p> <p>This attack uses ICMP to redirect the network router function to some other host. If that host can not provide router services, a DoS of network communications occurs as routing stops. This can also be modified to single out a specific system, so that only that system is subject to attack (because only that system sees the 'false' router). By providing router services from a compromised host, the attacker can also place themselves in a man-in-the-middle situation and take control of any open channel at will (as mentioned earlier, this is often used with TCP packet forgery and spoofing to intercept and change open TELNET sessions).</p> |



|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| router-solicit   | <p>Optional. Detects router solicitation attacks</p> <p>The ICMP router solicitation scan is used to actively find routers on a network. A hacker could set up a protocol analyzer to detect routers as they broadcast routing information on the network. In some instances, however, routers may not send updates. For example, if the local network does not have other routers, the router may be configured to not send routing information packets onto the local network. ICMP offers a method for router discovery. Clients send ICMP router solicitation multicasts onto the network, and routers must respond (as defined in RFC 1122). (For more information about the process of ICMP router solicitation, see "Routing Sequences for ICMP:")</p> <p>By sending ICMP router solicitation packets (ICMP type 9) on the network and listening for ICMP router discovery replies (ICMP type 10), hackers can build a list of all of the routers that exist on a network segment. Hackers often use this scan to locate routers that do not reply to ICMP echo requests.</p> |
| smurf            | <p>Optional. In this attack, a large number of ICMP echo packets are sent with a spoofed source address. This causes the device with the spoofed source address to be flooded with a large number of replies.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| snork            | <p>Optional. This attack causes a remote Windows™ NT to consume 100% of the CPU's resources. This attack uses a UDP packet with a destination port of 135 and a source port of 7, 9, or 135. This attack can also be exploited as a bandwidth consuming attack.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| tcp-bad-sequence | <p>Optional. A DoS attack that uses a specially crafted TCP packet to cause the targeted device to drop all subsequent network traffic for a specific TPC connection.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| tcp-fin-scan     | <p>Optional. Detects TCP FIN scan attacks</p> <p>Hackers use the TCP FIN scan to identify listening TCP port numbers based on how the target device reacts to a transaction close request for a TCP port (even though no connection may exist before these close requests are made). This type of scan can get through basic firewalls and boundary routers that filter on incoming TCP packets with the <i>Finish</i> (FIN) and ACK flag combination. The TCP packets used in this scan include only the TCP FIN flag setting.</p> <p>If the target device's TCP port is closed, the target device sends a TCP RST packet in reply. If the target device's TCP port is open, the target device discards the FIN and sends no reply.</p>                                                                                                                                                                                                                                                                                                                                             |

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| tcp-intercept            | <p>Optional. Prevents TCP intercept attacks by using TCP SYN cookies</p> <p>A SYN-flooding attack occurs when a hacker floods a server with a barrage of requests for connection.</p> <p>Because these messages have unreachable return addresses, the connections cannot be established. The resulting volume of unresolved open connections eventually overwhelms the server and can cause it to deny service to valid requests, thereby preventing legitimate users from connecting to a Web site, accessing email, using FTP service, and so on.</p> <p>The TCP intercept feature helps prevent SYN-flooding attacks by intercepting and validating TCP connection requests. In intercept mode, the TCP intercept software intercepts TCP SYN (synchronization ) packets from clients to servers that match an extended access list. The software establishes a connection with the client on behalf of the destination server, and if successful, establishes the connection with the server on behalf of the client and knits the two half-connections together transparently. Thus, connection attempts from unreachable hosts will never reach the server. The software continues to intercept and forward packets throughout the duration of the connection. The number of SYNs per second and the number of concurrent connections proxied depends on the platform, memory, processor, and other factors. In the case of illegitimate requests, the software's aggressive timeouts on half-open connections and its thresholds on TCP connection requests protect destination servers while still allowing valid requests.</p> <p>When establishing a security policy using TCP intercept, you can choose to intercept all requests or only those coming from specific networks or destined for specific servers. You can also configure the connection rate and threshold of outstanding connections. Optionally operate TCP intercept in watch mode, as opposed to intercept mode. In watch mode, the software passively watches the connection requests flowing through the router. If a connection fails to get established in a configurable interval, the software intervenes and terminates the connection attempt.</p> |
| tcp-null-scan            | <p>Optional. Detects TCP NULL scan attacks</p> <p>Hackers use the TCP NULL scan to identify listening TCP ports. This scan also uses a series of strangely configured TCP packets, which contain a sequence number of 0 and no flags. Again, this type of scan can get through some firewalls and boundary routers that filter incoming TCP packets with standard flag settings.</p> <p>If the target device's TCP port is closed, the target device sends a TCP RST packet in reply. If the target device's TCP port is open, the target discards the TCP NULL scan, sending no reply.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| tcp-post-syn             | <p>Optional. Detects TCP post SYN DoS attacks</p> <p>A remote attacker may be attempting to avoid detection by sending a SYN frame with a different sequence number than the original SYN. This can cause an Intrusion Detection System (IDS) to become unsynchronized with the data in a connection. Subsequent frames sent during the connection are ignored by the IDS.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| tcp-sequence-past-window | <p>Optional. Enables a TCP SEQUENCE PAST WINDOW DoS attack check. Disable this check to work around a bug in Windows XP's TCP stack which sends data past the window when conducting a selective ACK.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| tcp-xmas-scan            | <p>Optional. A TCP XMAS scan finds services on ports. A closed port returns a RST. This allows the attacker to identify open ports</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| tcphdrfrag               | <p>Optional. A DoS attack where the TCP header spans IP fragments</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| twinge                   | <p>Optional. A twinge attack is a flood of false ICMP packets to try and slow down a system</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| udp-short-hdr            | <p>Optional. Enables the identification of truncated UDP headers and UDP header length fields</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

|               |                                                                                                                                                                                                                                              |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| winnuke       | Optional. This DoS attack is specific to Windows™ 95 and Windows™ NT. The WINNUKE DoS attack sends a large amount of data to UDP port 137 to crash the NETBIOS service on windows and results in high CPU utilization on the target machine. |
| log-and-drop  | Logs the event and drops the packet                                                                                                                                                                                                          |
| log-only      | Logs the event only, the packet is not dropped                                                                                                                                                                                               |
| log-level     | Configures the log level                                                                                                                                                                                                                     |
| <0-7>         | Sets the numeric logging level                                                                                                                                                                                                               |
| emergencies   | Numerical severity 0. System is unusable                                                                                                                                                                                                     |
| alerts        | Numerical severity 1. Indicates a condition where immediate action is required                                                                                                                                                               |
| critical      | Numerical severity 2. Indicates a critical condition                                                                                                                                                                                         |
| errors        | Numerical severity 3. Indicates an error condition                                                                                                                                                                                           |
| warnings      | Numerical severity 4. Indicates a warning condition                                                                                                                                                                                          |
| notification  | Numerical severity 5. Indicates a normal but significant condition                                                                                                                                                                           |
| informational | Numerical severity 6. Indicates a informational condition                                                                                                                                                                                    |
| debugging     | Numerical severity 7. Debugging messages                                                                                                                                                                                                     |

```
ip dos {ascend/broadcast-multicast-icmp/chargen/fraggle/ftp-bounce/invalid-protocol/
ip-ttl-zero/ipsproof/land/option-route/router-advt/router-solicit/smurf/snork/tcp-bad-
sequence/
tcp-fin-scan/tcp-intercept/tcp-null-scan/tcp-post-scan/tcp-sequence-past-window/tcp-xmas-
scan/
tcphdrfrag/twinge/udp-short-hdr/winnuke} [drop-only]
```

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dos                      | Identifies IP events as DoS events                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| ascend                   | Optional. Enables an ASCEND DoS check. Ascend routers listen on UDP port 9 for packets from Ascend's Java Configurator. Sending a formatted packet to this port can cause an Ascend router to crash.                                                                                                                                                                                                                                                                                                   |
| broadcast-multicast-icmp | Optional. Detects broadcast or multicast ICMP packets as an attack                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| chargen                  | Optional. The chargen (Character Generation Protocol) is an IP suite service primarily used for testing and debugging networks. It is also used as a source of generic payload for bandwidth and QoS measurements.                                                                                                                                                                                                                                                                                     |
| fraggle                  | Optional. A Fraggle DoS attack checks for UDP packets to or from port 7 or 19                                                                                                                                                                                                                                                                                                                                                                                                                          |
| ftp-bounce               | Optional. A FTP bounce attack is a MIM attack that enables an attacker to open a port on a different machine using FTP. FTP requires that when a connection is requested by a client on the FTP port (21), another connection must open between the server and the client. To confirm, the PORT command has the client specify an arbitrary destination machine and port for the data connection. This is exploited by the attacker to gain access to a device that may not be the originating client. |
| invalid-protocol         | Optional. Enables a check for invalid protocol number                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| ip-ttl-zero              | Optional. Enables a check for the TCP/IP TTL field having a value of zero (0)                                                                                                                                                                                                                                                                                                                                                                                                                          |
| ipsproof                 | Optional. Enables a check for IP spoofing DoS attack                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

|                          |                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| land                     | Optional. A LAND (Local Area Network Denial) is a DoS attack where IP packets are spoofed and sent to a device where the source IP and destination IP of the packet are the target device's IP, and similarly, the source port and destination port are open ports on the same device. This causes the attacked device to reply to itself continuously. |
| option-route             | Optional. Enables an IP Option Record Route DoS check                                                                                                                                                                                                                                                                                                   |
| router-advrt             | Optional. This is an attack, where a default route entry is added remotely to a device. This route entry is given preference, and thereby exposes an attack vector.                                                                                                                                                                                     |
| router-solicit           | Optional. Router solicitation messages are sent to locate routers as a form of network scanning. This information can then be used to attack a device.                                                                                                                                                                                                  |
| smurf                    | Optional. In this attack, a large number of ICMP echo packets are sent with a spoofed source address. This causes the device with the spoofed source address to be flooded with a large number of replies.                                                                                                                                              |
| snork                    | Optional. This attack causes a remote Windows™ NT to consume 100% of the CPU's resources. This attack uses a UDP packet with a destination port of 135 and a source port of 7, 9, or 135. This attack can also be exploited as a bandwidth consuming attack.                                                                                            |
| tcp-bad-sequence         | Optional. A DoS attack that uses a specially crafted TCP packet to cause the targeted device to drop all subsequent network traffic for a specific TPC connection                                                                                                                                                                                       |
| tcp-fin-scan             | Optional. A FIN scan finds services on ports. A closed port returns a RST. This allows the attacker to identify open ports.                                                                                                                                                                                                                             |
| tcp-intercept            | Optional. Prevents TCP intercept attacks by using TCP SYN cookies                                                                                                                                                                                                                                                                                       |
| tcp-null-scan            | Optional. A TCP null scan finds services on ports. A closed port returns a RST. This allows the attacker to identify open ports                                                                                                                                                                                                                         |
| tcp-post-syn             | Optional. Enables a TCP post SYN DoS attack                                                                                                                                                                                                                                                                                                             |
| tcp-sequence-past-window | Optional. Enables a TCP SEQUENCE PAST WINDOW DoS attack check. Disable this check to work around a bug in Windows XP's TCP stack which sends data past the window when conducting a selective ACK.                                                                                                                                                      |
| tcp-xmas-scan            | Optional. A TCP XMAS scan finds services on ports. A closed port returns a RST. This allows the attacker to identify open ports.                                                                                                                                                                                                                        |
| tcphdrfrag               | Optional. A DoS attack where the TCP header spans IP fragments                                                                                                                                                                                                                                                                                          |
| twinge                   | Optional. A twinge attack is a flood of false ICMP packets to try and slow down a system                                                                                                                                                                                                                                                                |
| udp-short-hdr            | Optional. Enables the identification of truncated UDP headers and UDP header length fields                                                                                                                                                                                                                                                              |
| winnuke                  | Optional. This DoS attack is specific to Windows™ 95 and Windows™ NT, causing devices to crash with a blue screen                                                                                                                                                                                                                                       |
| drop-only                | Optional. Drops a packet without logging                                                                                                                                                                                                                                                                                                                |

```
ip dos tcp-max-incomplete [high|low] <1-1000>
```

|                    |                                                                           |
|--------------------|---------------------------------------------------------------------------|
| dos                | Identifies IP events as DoS events                                        |
| tcp-max-incomplete | Sets the limits for the maximum number of incomplete TCP connections      |
| high               | Sets the upper limit for the maximum number of incomplete TCP connections |
| low                | Sets the lower limit for the maximum number of incomplete TCP connections |
| <1-1000>           | Sets the range limit from 1 - 1000 connections                            |

```
ip tcp adjust-mss <472-1460>
```

|            |                                                                                        |
|------------|----------------------------------------------------------------------------------------|
| tcp        | Identifies and configures TCP events and configuration items                           |
| adjust-mss | Adjusts the TCP MSS. Use this option to adjust the MSS for TCP segments on the router. |
| <472-1460> | Sets the TCP MSS value from 472 - 1460 bytes. The default is 472 bytes.                |

```
ip tcp [optimize-unnecessary-resends|recreate-flow-on-out-of-state-syn|
validate-icmp-unreachable|validate-rst-ack-number|validate-rst-seq-number]
```

|                                    |                                                                                                                       |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| tcp                                | Identifies and configures TCP events and configuration items                                                          |
| optimize-unnecessary-resends       | Enables the validation of unnecessary TCP packets                                                                     |
| recreate-flow-on-out-of-state-sync | Allows a TCP SYN packet to delete an old flow in TCP_FIN_FIN_STATE, and TCP_CLOSED_STATE states and create a new flow |
| validate-icmp-unreachable          | Enables the validation of the sequence number in ICMP unreachable error packets, which abort an established TCP flow  |
| validate-rst-ack-number            | Enables the validation of the acknowledgment number in RST packets, which abort a TCP flow                            |
| validate-rst-seq-number            | Enables the validation of the sequence number in RST packets, which abort an established TCP flow                     |

### Examples

```
nx9500-6C8809(config-fw-policy-testFW)#ip dos fraggle drop-only
nx9500-6C8809(config-fw-policy-testFW)#ip dos tcp-max-incomplete high 600
nx9500-6C8809(config-fw-policy-testFW)#ip dos tcp-max-incomplete low 60
nx9500-6C8809(config-fw-policy-testFW)#ip dos tcp-sequence-past-window drop-only
nx9500-6C8809(config-fw-policy-testFW)#show context
firewall-policy testFW
 ip dos fraggle drop-only
 ip dos tcp-sequence-past-window drop-only
 ip dos tcp-max-incomplete high 600
 ip dos tcp-max-incomplete low 60
 flow timeout icmp 16000
 flow timeout udp 10000
 flow timeout tcp established 1500
 flow timeout other 16000
 dhcp-offer-convert
 alg facetime
 dns-snoop entry-timeout 1200
nx9500-6C8809(config-fw-policy-testFW)#
```

### Related Commands

|                 |                                      |
|-----------------|--------------------------------------|
| no on page 1510 | Resets firewall policy IP components |
|-----------------|--------------------------------------|

### ip-mac

Defines an action based on the device IP MAC table, and also detects conflicts between IP addresses and MAC addresses

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000

- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
ip-mac [conflict|routing]
ip-mac conflict drop-only
ip-mac conflict [log-and-drop|log-only] log-level [<0-7>|alerts|critical|debug|
emergencies|errors|informational|notifications|warnings]
ip-mac routing conflict drop-only
ip-mac routing conflict [log-and-drop|log-only] log-level [<0-7>|alerts|critical|debug|
emergencies|errors|informational|notifications|warnings]
```

### Parameters

```
ip-mac conflict drop-only
```

|           |                                                                                                                    |
|-----------|--------------------------------------------------------------------------------------------------------------------|
| conflict  | Action performed when a conflict exists between the IP address and MAC address. This option is enabled by default. |
| drop-only | Drops a packet without logging                                                                                     |

```
ip-mac conflict [log-and-drop|log-only] log-level [<0-7>|alerts|critical|debug|
emergencies|errors|informational|notifications|warnings]
```

|               |                                                                                                                    |
|---------------|--------------------------------------------------------------------------------------------------------------------|
| conflict      | Action performed when a conflict exists between the IP address and MAC address. This option is enabled by default. |
| log-and-drop  | Logs the event and drops the packet. This is the default setting.                                                  |
| log-only      | Logs the event only, the packet is not dropped                                                                     |
| log-level     | Configures the log level                                                                                           |
| <0-7>         | Sets the numeric logging level                                                                                     |
| alerts        | Numerical severity 1. Indicates a condition where immediate action is required                                     |
| critical      | Numerical severity 2. Indicates a critical condition                                                               |
| debugging     | Numerical severity 7. Debugging messages                                                                           |
| emergencies   | Numerical severity 0. System is unusable                                                                           |
| errors        | Numerical severity 3. Indicates an error condition                                                                 |
| informational | Numerical severity 6. Indicates a informational condition                                                          |
| notification  | Numerical severity 5. Indicates a normal but significant condition                                                 |
| warnings      | Numerical severity 4. Indicates a warning condition. This is the default setting.                                  |

```
ip-mac routing conflict drop-only
```

|           |                                                                                                                                                                                                           |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| routing   | Enables IPMAC routing conflict detection. This is also known as a Hole-196 attack in the network. This feature helps to detect if the client is sending routed packets to the correct router-mac-address. |
| conflict  | Defines the action performed when a routing table conflict is detected. This option is enabled by default.                                                                                                |
| drop-only | Drops a packet without logging                                                                                                                                                                            |

```
ip-mac routing conflict [log-and-drop|log-only] log-level [<0-7>|alerts|critical|debug|
emergencies|errors|informational|notifications|warnings]
```

|               |                                                                                                  |
|---------------|--------------------------------------------------------------------------------------------------|
| routing       | Defines a routing table based action                                                             |
| conflict      | Action performed when a conflict exists in the routing table. This option is enabled by default. |
| log-and-drop  | Logs the event and drops the packet. This is the default setting.                                |
| log-only      | Logs the event only, the packet is not dropped                                                   |
| log-level     | Configures the log level to log this event under                                                 |
| <0-7>         | Sets the numeric logging level                                                                   |
| alerts        | Numerical severity 1. Indicates a condition where immediate action is required                   |
| critical      | Numerical severity 2. Indicates a critical condition                                             |
| debugging     | Numerical severity 7. Debugging messages                                                         |
| emergencies   | Numerical severity 0. System is unusable                                                         |
| errors        | Numerical severity 3. Indicates an error condition                                               |
| informational | Numerical severity 6. Indicates a informational condition                                        |
| notification  | Numerical severity 5. Indicates a normal but significant condition                               |
| warnings      | Numerical severity 4. Indicates a warning condition. This is the default setting.                |

### Examples

```

nx9500-6C8809(config-fw-policy-testFW)#ip-mac conflict drop-only
nx9500-6C8809(config-fw-policy-testFW)#ip-mac routing conflict log-and-drop log-level
notifications
nx9500-6C8809(config-fw-policy-testFW)#show context
firewall-policy testFW
 ip dos fraggle drop-only
 ip dos tcp-sequence-past-window drop-only
 ip dos tcp-max-incomplete high 600
 ip dos tcp-max-incomplete low 60
 ip-mac conflict drop-only
 ip-mac routing conflict log-and-drop log-level notifications
 flow timeout icmp 16000
 flow timeout udp 10000
 flow timeout tcp established 1500
 flow timeout other 16000
 dhcp-offer-convert
 alg facetime
 dns-snoop entry-timeout 1200
nx9500-6C8809(config-fw-policy-testFW)#

```

### Related Commands

|                        |                                                                                               |
|------------------------|-----------------------------------------------------------------------------------------------|
| <b>no</b> on page 1510 | Disables actions based on device IP MAC table, IP address, and MAC address conflict detection |
|------------------------|-----------------------------------------------------------------------------------------------|

### ipv6

Configures IPv6 components on this firewall policy

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000

- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```

ipv6 [dos|duplicate-options|firewall|option|rewrite-flow-label|routing-type|
strict-ext-hdr-check|unknown-options]
ipv6 dos {hop-limit-zero/multicast-icmpv6/tcp-intercept-mobility} [drop-only|
log-and-drop|log-only]
ipv6 [duplicate-options|routing-type [one|two]|strict-ext-hdr-check|unknown-options]
[drop-only|log-and-drop|log-only]
ipv6 option {endpoint-identification/network-service-access-point/router-alert/
strict-hao-opt-alert/strict-padding} [drop-only|log-and-drop|log-only]
ipv6 [firewall enable|rewrite-flow-label]

```

## Parameters

```

ipv6 dos {hop-limit-zero/multicast-icmpv6/tcp-intercept-mobility}
[drop-only|log-and-drop|log-only]

```

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dos                    | Identifies IPv6 events as DoS events                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| hop-limit-zero         | Optional. Enables checking of IPv6 hop limit field. If the IPv6 hop limit field is ZERO (0) it is considered as attack. This option is enabled by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| multicast-icmpv6       | Optional. Enables detection of multicast ICMPv6 traffic as attack. This option is applicable only to ICMPv6 Echo request or reply packets. This option is enabled by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| tcp-intercept-mobility | Optional. Enables detection of IPv6 TCP packets with mobility option "HAO(Home-Address-Option)" or "RH(Routing Header) type two". When enabled, this option also detects the "don't generate TCP syn cookies" for such packets. This option is enabled by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| drop-only              | This parameter is common to all of the above keywords. Drops all packets. Drops the specified packet type (hop-limit-zero, multicast-icmpv6, and tcp-intercept-mobility).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| log-and-drop           | Logs the event and drops the packet. Drops the specified packet type (hop-limit-zero, multicast-icmpv6, and tcp-intercept-mobility) and logs an event.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| log-only               | Logs the event only, the packet is not dropped. Does not drop the specified packet type (hop-limit-zero, multicast-icmpv6, and tcp-intercept-mobility). But, an event is logged.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| log-level              | If selecting the "log-and-drop" and "log-only" action type, specify the log level. The options are: <ul style="list-style-type: none"> <li>• &lt;0-7&gt; – Sets the numeric logging level</li> <li>• alerts – Numerical severity 1. Indicates a condition where immediate action is required</li> <li>• critical – Numerical severity 2. Indicates a critical condition</li> <li>• debugging – Numerical severity 7. Debugging messages</li> <li>• emergencies – Numerical severity 0. System is unusable</li> <li>• errors – Numerical severity 3. Indicates an error condition</li> <li>• informational – Numerical severity 6. Indicates a informational condition</li> <li>• notifications – Numerical severity 5. Indicates a normal but significant condition</li> <li>• warnings – Numerical severity 4. Indicates a warning condition. This is the default setting.</li> </ul> |

```

ipv6 [duplicate-options|routing-type [one|two]|strict-ext-hdr-check|unknown-options]
[drop-only|log-and-drop|log-only]

```



|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| duplicate-options      | Enables handling of duplicate options in hop-by-hop and destination option extension headers. This configuration excludes HAO handling. This option is enabled by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| routing-type [one two] | Enables checking of the following IPv6 routing types: <ul style="list-style-type: none"> <li>• one – Routing Type 1(Nimrod routing). This option is disabled by default.</li> <li>• two – Routing Type 2(Mobile IP). This option is disabled by default.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| strict-ext-hdr-check   | Enables strict checking for out of order and number of occurrences of extension header. This option is enabled by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| unknown-options        | Enables handling unknown options in hop-by-hop and destination option extension headers. This option is enabled by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| drop-only              | This parameter is common to all of the above keywords.<br>Drops all packets. Drops the packet if matching any of the above specified types.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| log-and-drop           | Logs the event and drops the packet. Drops the packet, if matching any of the above specified types, and logs an event.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| log-only               | Logs the event only, the packet is not dropped. Does not drop the packet, if matching any of the above specified types. But an event is logged.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| log-level              | If selecting the “log-and-drop” and “log-only” action type, specify the log level. The options are: <ul style="list-style-type: none"> <li>• &lt;0-7&gt; – Sets the numeric logging level</li> <li>• alerts – Numerical severity 1. Indicates a condition where immediate action is required</li> <li>• critical – Numerical severity 2. Indicates a critical condition</li> <li>• debugging – Numerical severity 7. Debugging messages</li> <li>• emergencies – Numerical severity 0. System is unusable</li> <li>• errors – Numerical severity 3. Indicates an error condition</li> <li>• informational – Numerical severity 6. Indicates a informational condition</li> <li>• notifications – Numerical severity 5. Indicates a normal but significant condition</li> <li>• warnings – Numerical severity 4. Indicates a warning condition. This is the default setting.</li> </ul> |

*ipv6 option {endpoint-identification|network-service-access-point/router-alert/strict-hao-opt-alert/strict-padding} [drop-only|log-and-drop|log-only*

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| option       | Enables checking for the following ipv6 extension header options: <ul style="list-style-type: none"> <li>• End point identification option (disabled by default)</li> <li>• Network service access point address option (disabled by default)</li> <li>• Router alert option (disabled by default)</li> <li>• Home address option in destination option extension header (enabled by default)</li> <li>• Pad1 and PadN options validating (enabled by default)</li> </ul> <p>All of these are optional parameters. If no option is specified, the system enables checks as per the default values.</p> |
| drop-only    | This parameter is common to all of the above keywords.<br>Drops all packets. Drops the packet if matching any of the above specified “option” types.                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| log-and-drop | Logs the event and drops the packet. Drops the packet, if matching any of the above specified “option” types, and logs an event.                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| log-only  | Logs the event only, the packet is not dropped. Does not drop the packet, if matching any of the above specified “option” types. But an event is logged.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| log-level | <p>If selecting the “log-and-drop” and “log-only” action type, specify the log level. The options are:</p> <ul style="list-style-type: none"> <li>• &lt;0-7&gt; – Sets the numeric logging level</li> <li>• alerts – Numerical severity 1. Indicates a condition where immediate action is required</li> <li>• critical – Numerical severity 2. Indicates a critical condition</li> <li>• debugging – Numerical severity 7. Debugging messages</li> <li>• emergencies – Numerical severity 0. System is unusable</li> <li>• errors – Numerical severity 3. Indicates an error condition</li> <li>• informational – Numerical severity 6. Indicates a informational condition</li> <li>• notifications – Numerical severity 5. Indicates a normal but significant condition</li> <li>• warnings – Numerical severity 4. Indicates a warning condition. This is the default setting.</li> </ul> |

```
ipv6 [firewall enable|rewrite-flow-label]
```

|                    |                                                                                         |
|--------------------|-----------------------------------------------------------------------------------------|
| firewall enable    | Enables IPv6 firewall. This option is enabled by default.                               |
| rewrite-flow-label | Rewrites the IPv6 flow label field of every packet. This option is disabled by default. |

### Examples

```

nx9500-6C8809(config-fw-policy-testFW)#ipv6 dos hop-limit-zero drop-only
nx9500-6C8809(config-fw-policy-testFW)#ipv6 routing-type two log-and-drop log-level
warnings
nx9500-6C8809(config-fw-policy-testFW)#show context
firewall-policy testFW
 ip dos fraggle drop-only
 ip dos tcp-sequence-past-window drop-only
 ip dos tcp-max-incomplete high 600
 ip dos tcp-max-incomplete low 60
 ip-mac conflict drop-only
 ip-mac routing conflict log-and-drop log-level notifications
 flow timeout icmp 16000
 flow timeout udp 10000
 flow timeout tcp established 1500
 flow timeout other 16000
 dhcp-offer-convert
 ipv6 routing-type two log-and-drop log-level warnings
 ipv6 dos hop-limit-zero drop-only
 alg facetime
 dns-snoop entry-timeout 1200
nx9500-6C8809(config-fw-policy-testFW)#

```

### Related Commands

|                        |                                               |
|------------------------|-----------------------------------------------|
| <b>no</b> on page 1510 | Resets this firewall policy’s IPv6 components |
|------------------------|-----------------------------------------------|

### *ipv6-mac*

Defines an action based on conflicts detected in a device’s IPv6 and MAC addresses

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
ipv6-mac [conflict|routing]
ipv6-mac conflict [drop-only|log-and-drop|log-only]
ipv6-mac routing conflict [drop-only|log-and-drop|log-only]
```

### Parameters

```
ipv6-mac conflict [drop-only|log-and-drop|log-only]
```

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| conflict     | Enables detection of conflict between a device's IPv6 and MAC addresses. This option is enabled by default. This command also specifies the action to be performed when a such a conflict is detected. The options are: drop-only, log-and-drop, and log-only.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| drop-only    | Drops a packet (with conflicting IPv6 and MAC address) without logging                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| log-and-drop | Logs the event and drops the packet. This is the default setting.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| log-only     | Logs the event only, the packet is not dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| log-level    | If selecting the "log-and-drop" and "log-only" action type, specify the log level. The options are: <ul style="list-style-type: none"><li>• &lt;0-7&gt; – Sets the numeric logging level</li><li>• alerts – Numerical severity 1. Indicates a condition where immediate action is required</li><li>• critical – Numerical severity 2. Indicates a critical condition</li><li>• debugging – Numerical severity 7. Debugging messages</li><li>• emergencies – Numerical severity 0. System is unusable</li><li>• errors – Numerical severity 3. Indicates an error condition</li><li>• informational – Numerical severity 6. Indicates a informational condition</li><li>• notifications – Numerical severity 5. Indicates a normal but significant condition</li><li>• warnings – Numerical severity 4. Indicates a warning condition. This is the default setting.</li></ul> |

```
ipv6-mac routing conflict [drop-only|log-and-drop|log-only]
```

|                  |                                                                                                                                                                                                                                                                    |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| routing conflict | Enables detection of conflict between the next-hop's IPv6 and MAC addresses. This option is enabled by default. This command also specifies the action to be performed when a such a conflict is detected. The options are: drop-only, log-and-drop, and log-only. |
| drop-only        | Drops a packet (with conflicting next-hop IPv6 and MAC addresses) without logging                                                                                                                                                                                  |
| log-and-drop     | Logs the event and drops the packet. This is the default setting.                                                                                                                                                                                                  |

|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| log-only  | Logs the event only, the packet is not dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| log-level | <p>If selecting the “log-and-drop” and “log-only” action type, specify the log level. The options are:</p> <ul style="list-style-type: none"> <li>• &lt;0-7&gt; – Sets the numeric logging level</li> <li>• alerts – Numerical severity 1. Indicates a condition where immediate action is required</li> <li>• critical – Numerical severity 2. Indicates a critical condition</li> <li>• debugging – Numerical severity 7. Debugging messages</li> <li>• emergencies – Numerical severity 0. System is unusable</li> <li>• errors – Numerical severity 3. Indicates an error condition</li> <li>• informational – Numerical severity 6. Indicates a informational condition</li> <li>• notifications – Numerical severity 5. Indicates a normal but significant condition</li> <li>• warnings – Numerical severity 4. Indicates a warning condition. This is the default setting.</li> </ul> |

### Examples

```

nx9500-6C8809(config-fw-policy-testFW)#ipv6-mac routing conflict drop-only
nx9500-6C8809(config-fw-policy-testFW)#show context
firewall-policy testFW
 ip dos fraggle drop-only
 ip dos tcp-sequence-past-window drop-only
 ip dos tcp-max-incomplete high 600
 ip dos tcp-max-incomplete low 60
 ip-mac conflict drop-only
 ip-mac routing conflict log-and-drop log-level notifications
 flow timeout icmp 16000
 flow timeout udp 10000
 flow timeout tcp established 1500
 flow timeout other 16000
 dhcp-offer-convert
 ipv6 routing-type two log-and-drop log-level warnings
 ipv6 dos hop-limit-zero drop-only
 alg facetime
 dns-snoop entry-timeout 1200
 ipv6-mac routing conflict drop-only
nx9500-6C8809(config-fw-policy-testFW)#

```

### Related Commands

|                              |                                                                   |
|------------------------------|-------------------------------------------------------------------|
| <code>no</code> on page 1510 | Disables actions based on IPv6 and MAC address conflict detection |
|------------------------------|-------------------------------------------------------------------|

### logging

Configures enhanced firewall logging

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
logging [icmp-all|icmp-packet-drop|malformed-packet-drop|verbose]
logging icmp-all
logging verbose
logging [icmp-packet-drop|malformed-packet-drop] [all|rate-limited]
```

## Parameters

```
logging icmp-all
```

|          |                                                                                                       |
|----------|-------------------------------------------------------------------------------------------------------|
| logging  | Configures enhanced firewall logging parameters                                                       |
| icmp-all | Enables logging of all ICMPv4/v6 packets allowed by the firewall. This option is disabled by default. |

```
logging verbose
```

|         |                                                                           |
|---------|---------------------------------------------------------------------------|
| logging | Configures enhanced firewall logging. This option is disabled by default. |
| verbose | Enables verbose logging                                                   |

```
logging [icmp-packet-drop|malformed-packet-drop] [all|rate-limited]
```

|                       |                                                                                                                 |
|-----------------------|-----------------------------------------------------------------------------------------------------------------|
| logging               | Configures enhanced firewall logging                                                                            |
| icmp-packet-drop      | Enables logging of ICMP (ICMPv4 and ICMPv6) packets that do not pass sanity checks. The default is none.        |
| malformed-packet-drop | Enables logging of raw IP (IPv4 and IPv6) packets that do not pass sanity checks. The default is none.          |
| all                   | Logs all messages                                                                                               |
| rate-limited          | Enables rate-limited logging. This option sets the rate limit for log messages to one message every 20 seconds. |

## Examples

```
nx9500-6C8809(config-fw-policy-testFW)#logging verbose
nx9500-6C8809(config-fw-policy-testFW)#logging icmp-packet-drop rate-limited
nx9500-6C8809(config-fw-policy-testFW)#logging malformed-packet-drop all
nx9500-6C8809(config-fw-policy-testFW)#show context
firewall-policy testFW
 ip dos fraggle drop-only
 ip dos tcp-sequence-past-window drop-only
 ip dos tcp-max-incomplete high 600
 ip dos tcp-max-incomplete low 60
 ip-mac conflict drop-only
 ip-mac routing conflict log-and-drop log-level notifications
 flow timeout icmp 16000
 flow timeout udp 10000
 flow timeout tcp established 1500
 flow timeout other 16000
 dhcp-offer-convert
 ipv6 routing-type two log-and-drop log-level warnings
 ipv6 dos hop-limit-zero drop-only
 alg facetime
 logging icmp-packet-drop rate-limited
 logging malformed-packet-drop all
 logging verbose
 dns-snoop entry-timeout 1200
```

```
ipv6-mac routing conflict drop-only
nx9500-6C8809(config-fw-policy-testFW)#
nx9500-6C8809(config-fw-policy-test2)#show context
firewall-policy test2
 no ip dos tcp-sequence-past-window
nx9500-6C8809(config-fw-policy-test2)#
nx9500-6C8809(config-fw-policy-test2)#logging icmp-all
nx9500-6C8809(config-fw-policy-test2)#show context
firewall-policy test2
 no ip dos tcp-sequence-past-window
 logging icmp-all
nx9500-6C8809(config-fw-policy-test2)
```

### Related Commands

`no` on page 1510

Disables enhanced firewall logging

### *proxy-arp*

Enables the generation of ARP responses on behalf of another device. Proxy ARP allows the Firewall to handle ARP routing requests for devices behind the firewall. This option is enabled by default.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
proxy-arp
```

#### Parameters

None

#### Examples

```
nx9500-6C8809(config-fw-policy-test)#proxy-arp
nx9500-6C8809(config-fw-policy-testFW)#show context include-factory | include proxy-arp
 proxy-arp
nx9500-6C8809(config-fw-policy-testFW)#
```

### Related Commands

`no` on page 1510

Disables the generation of ARP responses on behalf of another device

### *proxy-nd*

Enables generation of ND responses (for IPv6) on behalf of another device

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000

- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

proxy-nd

### Parameters

None

### Examples

```
nx9500-6C8809(config-fw-policy-testFW)#proxy-nd
nx9500-6C8809(config-fw-policy-testFW)#show context include-factory | include proxy-nd
proxy-nd
nx9500-6C8809(config-fw-policy-testFW)#
```

### Related Commands

|                 |                                                                     |
|-----------------|---------------------------------------------------------------------|
| no on page 1510 | Disables the generation of ND responses on behalf of another device |
|-----------------|---------------------------------------------------------------------|

## *stateful-packet-inspection-12*

Enables layer 2 firewall stateful packet inspection. When enabled, allows stateful packet inspection for RF Domain manager routed interfaces within the layer 2 firewall. This option is enabled by default.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

stateful-packet-inspection-12

### Parameters

None

### Examples

```
nx9500-6C8809(config-fw-policy-testFW)#stateful-packet-inspection-12
```

### Related Commands

|                 |                                                           |
|-----------------|-----------------------------------------------------------|
| no on page 1510 | Disables stateful packet inspection in a layer 2 firewall |
|-----------------|-----------------------------------------------------------|

## *storm-control*

Enables storm control on the firewall policy

Storms are packet bombardments that exceed the high threshold value configured for an interface. During a storm, packets are throttled until the rate falls below the configured rate, severely impacting performance for the RF Domain manager interface.

Storm control limits multicast, unicast and broadcast frames accepted and forwarded by a device. Messages are logged based on their severity level.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
storm-control [arp|broadcast|multicast|unicast]
storm-control [arp|broadcast|multicast|unicast] [level|log]
storm-control [arp|broadcast|multicast|unicast] level <1-1000000>
[fe <1-4>|ge <1-8>|port-channel <1-8>|up1|wlan <WLAN-NAME>]
storm-control [arp|broadcast|multicast|unicast] log [<0-7>|alerts|critical|
debugging|emergencies|errors|informational|none|notifications|warnings]
```

### Parameters

```
storm-control [arp|broadcast|multicast|unicast] level <1-1000000>
[fe <1-4>|ge <1-8>|port-channel <1-8>|up1|wlan <WLAN-NAME>]
```

|                    |                                                                                                                                                                                                                 |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| arp                | Configures storm control for ARP packets                                                                                                                                                                        |
| broadcast          | Configures storm control for broadcast packets                                                                                                                                                                  |
| multicast          | Configures storm control for multicast packets                                                                                                                                                                  |
| unicast            | Configures storm control for unicast packets                                                                                                                                                                    |
| level <1-1000000>  | Configures the allowed number of packets received per second before storm control begins <ul style="list-style-type: none"> <li>• &lt;1-1000000&gt; - Sets the number of packets received per second</li> </ul> |
| fe <1-4>           | Sets the FastEthernet port for storm control from 1 - 4                                                                                                                                                         |
| ge <1-8>           | Sets the GigabitEthernet port for storm control from 1 - 8                                                                                                                                                      |
| port-channel <1-8> | Sets the port channel for storm control from 1- 8                                                                                                                                                               |
| up1                | Sets the uplink interface                                                                                                                                                                                       |
| wlan <WLAN-NAME>   | Configures the WLAN <ul style="list-style-type: none"> <li>• &lt;WLAN-NAME&gt; - Sets the WLAN ID for the storm control configuration</li> </ul>                                                                |

```
storm-control [arp|bcast|multicast|unicast] log [<0-7>|alerts|critical|debugging|
emergencies|errors|informational|none|notifications|warnings]
```

|           |                                                                                |
|-----------|--------------------------------------------------------------------------------|
| arp       | Configures storm control for ARP packets                                       |
| broadcast | Configures storm control for broadcast packets                                 |
| multicast | Configures storm control for multicast packets                                 |
| unicast   | Configures storm control for unicast packets                                   |
| log       | Configures the storm control log level for storm control events                |
| <0-7>     | Sets the numeric logging level from 0 - 7                                      |
| alerts    | Numerical severity 1. Indicates a condition where immediate action is required |



|               |                                                                    |
|---------------|--------------------------------------------------------------------|
| critical      | Numerical severity 2. Indicates a critical condition               |
| debugging     | Numerical severity 7. Debugging messages                           |
| emergencies   | Numerical severity 0. System is unusable                           |
| errors        | Numerical severity 3. Indicates an error condition                 |
| informational | Numerical severity 6. Indicates a informational condition          |
| none          | Disables storm control logging                                     |
| notification  | Numerical severity 5. Indicates a normal but significant condition |
| warnings      | Numerical severity 4. Indicates a warning condition                |

### Examples

```

nx9500-6C8809(config-fw-policy-testFW)#storm-control arp log warnings
nx9500-6C8809(config-fw-policy-testFW)#storm-control broadcast level 2
nx9500-6C8809(config-fw-policy-testFW)#show context
firewall-policy testFW
 ip dos fraggle drop-only
 ip dos tcp-sequence-past-window drop-only
 ip dos tcp-max-incomplete high 600
 ip dos tcp-max-incomplete low 60
 storm-control broadcast level 20000 ge 4
 storm-control arp log warnings
 ip-mac conflict drop-only
 ip-mac routing conflict log-and-drop log-level notifications
 flow timeout icmp 16000
 flow timeout udp 10000
 flow timeout tcp established 1500
 flow timeout other 16000
 dhcp-offer-convert
 ipv6 routing-type two log-and-drop log-level warnings
 ipv6 dos hop-limit-zero drop-only
 alg facetime
 logging icmp-packet-drop rate-limited
 logging malformed-packet-drop all
 logging verbose
 dns-snoop entry-timeout 1200
 ipv6-mac routing conflict drop-only
nx9500-6C8809(config-fw-policy-testFW)#

```

### Related Commands

|                        |                                                                                                              |
|------------------------|--------------------------------------------------------------------------------------------------------------|
| <b>no</b> on page 1510 | Disables storm control limits on multicast, unicast, and broadcast frames accepted and forwarded by a device |
|------------------------|--------------------------------------------------------------------------------------------------------------|

### *virtual-defragmentation*

Enables the virtual de-fragmentation of IPv4 and IPv6 packets. This parameter is required for optimal firewall functionality and is enabled by default.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
virtual-defragmentation {maximum-defragmentation-per-host <1-16384>|
maximum-fragments-per-datagram <2-8129>|minimum-first-fragment-length <8-1500>|timeout
<1-60>}
```

## Parameters

```
virtual-defragmentation {maximum-defragmentation-per-host <1-16384>|
maximum-fragments-per-datagram <2-8129>|minimum-first-fragment-length <8-1500>|timeout
<1-60>}
```

|                                            |                                                                                                                                                                                                                                                                    |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| maximum-defragmentation-per-host <1-16384> | Optional. Configures the maximum number of active de-fragmentations allowed per host before it is dropped (applicable to IPv4 and IPV6 packets) <ul style="list-style-type: none"><li>• &lt;1-16384&gt; - Sets a value from 1 - 16384. The default is 8.</li></ul> |
| maximum-fragments-per-datagram <2-8129>    | Optional. Configures the maximum number of fragments allowed in a datagram before it is dropped (applicable to IPv4 and IPV6 packets) <ul style="list-style-type: none"><li>• &lt;2-8129&gt; - Sets a value from 2 - 8129. The default is 140.</li></ul>           |
| minimum-first-fragment-length <8-1500>     | Optional. Defines the minimum length required for the first fragment (applicable to IPv4 and IPV6 packets) <ul style="list-style-type: none"><li>• &lt;8-1500&gt; - Sets a value from 8 - 1500 bytes. The default is 8 bytes.</li></ul>                            |
| timeout <1-60>                             | Optional. Configures a virtual de-fragmentation timeout, in seconds, applicable to both IPv4 and IPV6 packets <ul style="list-style-type: none"><li>• &lt;1-60&gt; - Specify a value from 1 - 60 seconds. The default is 1 second.</li></ul>                       |

## Examples

```
nx9500-6C8809(config-fw-policy-testFW)#virtual-defragmentation maximum-fragments-per-
datagram 10
nx9500-6C8809(config-fw-policy-testFW)#virtual-defragmentation minimum-first-fragment-
length 100
nx9500-6C8809(config-fw-policy-testFW)#show context include-factory | include virtual-
defragmentation
virtual-defragmentation
virtual-defragmentation minimum-first-fragment-length 100
virtual-defragmentation maximum-fragments-per-datagram 10
virtual-defragmentation maximum-defragmentation-per-host 8
virtual-defragmentation timeout 1
nx9500-6C8809(config-fw-policy-testFW)#
```

## Related Commands

|                              |                                                             |
|------------------------------|-------------------------------------------------------------|
| <code>no</code> on page 1510 | Resets values or disables virtual d-efragmentation settings |
|------------------------------|-------------------------------------------------------------|

*no*

Negates a command or sets the default for firewall policy commands

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
no [acl-logging|alg|clamp|dhcp-offer-convert|dns-snoop|firewall|flow|ip|ip-mac|
ipv6|ipv6-mac|logging|proxy-arp|proxy-nd|stateful-packet-inspection-l2|storm-control|
virtual-defragmentation]
no [acl-logging|dhcp-offer-convert|proxy-arp|proxy-nd|stateful-packet-inspection-l2]
no alg [dns|facetime|ftp|sccp|sip|tftp]
no clamp tcp-mss
no dns-snoop entry-timeout
no firewall enable
no flow dhcp stateful
no flow timeout [icmp|other|udp]
no flow timeout tcp [closed-wait|established|reset|setup|stateless-fin-or-reset|
stateless-general]
no ip dos {ascend|broadcast-multicast-icmp/chargen/fraggle/ftp-bounce/invalid-protocol/
ip-ttl-zero/ipsproof/land/option-route/router-advrt/router-solicit/smurf/snork/tcp-bad-
sequence/
tcp-fin-scan/tcp-intercept/tcp-null-scan/tcp-post-syn/tcp-sequence-past-window/tcp-xmas-
scan/
tcphdrfrag/twinge/udp-short-hdr/winnuke}
no ip tcp [adjust-mss|optimize-unnecessary-resends|recreate-flow-on-out-of-state-syn|
validate-icmp-unreachable|validate-rst-ack-number|validate-rst-seq-number]
no ip-mac conflict
no ip-mac routing conflict
no ipv6 [dos|duplicate-options|firewall|option|rewrite-flow-label|routing-type|
strict-ext-hdr-check|unknown-options]
no ipv6 dos {hop-limit-zero/multicast-icmpv6/tcp-intercept-mobility}
no ipv6 [duplicate-options|routing-type [one|two]|strict-ext-hdr-check|unknown-options]
no ipv6 option {endpoint-identification/network-service-access-point/router-alert/
strict-hao-opt-alert/strict-padding}
no ipv6 [firewall enable|rewrite-flow-label]
no logging [icmp-all|icmp-packet-drop|verbose|malformed-packet-drop]
no storm-control [arp|broadcast|multicast|unicast] {fe <1-4>/ge <1-8>/log/
port-channel <1-8>/up1/wlan <WLAN-NAME>}
no virtual-defragmentation {maximum-fragments-per-datagram/minimum-first-fragment-length/
maximum-defragmentation-per-host/timeout}
```

## Parameters

```
no <PARAMETERS>
```

|                 |                                                                             |
|-----------------|-----------------------------------------------------------------------------|
| no <PARAMETERS> | Removes this firewall policy settings or reverts settings to default value. |
|-----------------|-----------------------------------------------------------------------------|

## Examples

The following example shows the firewall policy 'test' settings before the 'no' command are executed:

```
nx9500-6C8809(config-fw-policy-testFW)#show context
firewall-policy testFW
 ip dos fraggle drop-only
 ip dos tcp-sequence-past-window drop-only
 ip dos tcp-max-incomplete high 600
 ip dos tcp-max-incomplete low 60
 storm-control broadcast level 20000 ge 4
 storm-control arp log warnings
 ip-mac conflict drop-only
 ip-mac routing conflict log-and-drop log-level notifications
 flow timeout icmp 16000
 flow timeout udp 10000
 flow timeout tcp established 1500
 flow timeout other 16000
 dhcp-offer-convert
 ipv6 routing-type two log-and-drop log-level warnings
 ipv6 dos hop-limit-zero drop-only
 alg facetime
```

```

logging icmp-packet-drop rate-limited
logging malformed-packet-drop all
logging verbose
virtual-defragmentation minimum-first-fragment-length 100
virtual-defragmentation maximum-fragments-per-datagram 10
dns-snoop entry-timeout 1200
ipv6-mac routing conflict drop-only
nx9500-6C8809(config-fw-policy-testFW)#
nx9500-6C8809nx9500-6C8809(config-fw-policy-testFW)#no ip dos fraggle
nx9500-6C8809(config-fw-policy-testFW)#no storm-control arp log
nx9500-6C8809(config-fw-policy-testFW)#no dhcp-offer-convert
nx9500-6C8809(config-fw-policy-testFW)#no logging malformed-packet-drop

```

The following example shows the firewall policy 'test' settings after the 'no' commands are executed:

```

nx9500-6C8809(config-fw-policy-testFW)#show context
firewall-policy testFW
no ip dos fraggle
ip dos tcp-sequence-past-window drop-only
ip dos tcp-max-incomplete high 600
ip dos tcp-max-incomplete low 60
storm-control broadcast level 20000 ge 4
storm-control arp log none
ip-mac conflict drop-only
ip-mac routing conflict log-and-drop log-level notifications
flow timeout icmp 16000
flow timeout udp 10000
flow timeout tcp established 1500
flow timeout other 16000
ipv6 routing-type two log-and-drop log-level warnings
ipv6 dos hop-limit-zero drop-only
alg facetime
logging icmp-packet-drop rate-limited
logging verbose
virtual-defragmentation minimum-first-fragment-length 100
virtual-defragmentation maximum-fragments-per-datagram 10
dns-snoop entry-timeout 1200
ipv6-mac routing conflict drop-only
nx9500-6C8809(config-fw-policy-testFW)#

```

# MiNT Security Policy

## MINT-POLICY

---

This chapter summarizes MiNT policy commands in the CLI command structure.

All communication using the MiNT transport layer can be optionally secured. This includes confidentiality, integrity and authentication of all communications. In addition, a device can be configured to communicate over MiNT with other devices authorized by an administrator.

Use the (config) instance to configure mint-policy related configuration commands. To navigate to the config MiNT policy instance, use the following command:

```
<DEVICE>(config)#mint-policy global-default
nx9500-6C8809(config-mint-policy-global-default)#?
Mint Policy Mode commands:
 level Mint routing level
 lsp LSP
 mtu Configure the global Mint MTU
 no Negate a command or set its defaults
 router Mint router
 udp Configure mint UDP/IP encapsulation

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-mint-policy-global-default)#
```

### mint-policy-commands

The following table summarizes MiNT policy configuration commands:

**Table 46: MiNT-Policy Config Mode Commands**

| Command                             | Description                                                                      |
|-------------------------------------|----------------------------------------------------------------------------------|
| <a href="#">level</a> on page 1514  | Configures the MiNT routing level                                                |
| <a href="#">lsp</a> on page 1515    | Enables adding of checksum to LSP messages forwarded across MiNT links           |
| <a href="#">mtu</a> on page 1515    | Configures the global MiNT MTU                                                   |
| <a href="#">router</a> on page 1516 | Configures the priority for MiNT router packets (HELLO, LSP, PSNP, and EXT VLAN) |

**Table 46: MiNT-Policy Config Mode Commands (continued)**

| Command                       | Description                                         |
|-------------------------------|-----------------------------------------------------|
| <code>udp</code> on page 1517 | Configures the MiNT UDP/IP encapsulation parameters |
| <code>no</code> on page 1517  | Negates a command or sets its default               |

**Note**

For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see [COMMON COMMANDS](#) on page 640.

**Note**

The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (\_) character. In other words, the name of a device cannot contain an underscore.

*level*

Configures the global MiNT routing level

**Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

**Syntax**

```
level 2 area-id <1-16777215>
```

**Parameters**

```
level 2 area-id <1-16777215>
```

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>level 2</code>                    | Configures level 2 inter-site MiNT routing                                                                                                                                                                                                                                                                                                                                                               |
| <code>area-id &lt;1-16777215&gt;</code> | Configures the routing area identifier <ul style="list-style-type: none"> <li>• <code>&lt;1-16777215&gt;</code> – Specify a value from 1 - 16777215.</li> </ul> <p>The level 2 area ID is the global MiNT area identifier. This area identifier separates two overlapping MiNT networks. Configure the level 2 area ID only if there are two MiNT networks sharing the same packet broadcast domain.</p> |

**Examples**

```
nx9500-6C8809(config-mint-policy-global-default)#level 2 area-id 2000
nx9500-6C8809(config-mint-policy-global-default)#show context
mint-policy global-default
 level 2 area-id 2000
nx9500-6C8809(config-mint-policy-global-default)#
```

**Related Commands**

|                              |                                                                  |
|------------------------------|------------------------------------------------------------------|
| <code>no</code> on page 1517 | Disables level 2 MiNT packet routing (inter-site packet routing) |
|------------------------------|------------------------------------------------------------------|

## *lsp*

Enables adding of checksum to LSP (label-switched path) messages forwarded across MiNT links. When enabled, this option helps to verify integrity of LSP messages. LSP messages exchanged over MiNT links are often corrupted. These LSP corruptions cause inaccuracies in the SPF (Shortest Path First) calculation process, leading to access point adoption related issues. Enabling LSP checksum helps troubleshooting adoption-related issues.

### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### **Syntax**

```
lsp checksum
```

### **Parameters**

```
lsp checksum
```

|              |                                                                                                                                                                                                                                                                                     |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| lsp checksum | Enables adding of checksum to LSP messages forwarded across MiNT links. When enabled, the integrity of LSP messages is verified by matching the LSP message checksum at the MiNT link end nodes. In case of a match the message is uncorrupted. This option is disabled by default. |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### **Examples**

```
nx9500-6C8809(config-mint-policy-global-default)#lsp checksum
nx9500-6C8809(config-mint-policy-global-default)#show context
mint-policy global-default
 lsp checksum
nx9500-6C8809(config-mint-policy-global-default)#
```

### **Related Commands**

|                 |                                                                         |
|-----------------|-------------------------------------------------------------------------|
| no on page 1517 | Disables adding of checksum to LSP messages forwarded across MiNT links |
|-----------------|-------------------------------------------------------------------------|

## *mtu*

Configures global MiNT MTU (Multiple Transmission Unit). Use this command to specify the maximum packet size, in bytes, for MiNT routing. Higher the MTU values, greater is the network efficiency. The user data per packet increases, while protocol overheads, such as headers or underlying per-packet delays remain the same.

### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
mtu <900-1500>
```

## Parameters

```
mtu <900-1500>
```

|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mtu <900-1500> | Specifies the maximum packet size from 900 - 1500 bytes<br>The maximum packet size specified is rounded down to a value using the following formula: 4 + a multiple of 8.<br>The MTU setting specifies the maximum packet size used for MiNT packets. Larger packets are fragmented to fit within the specified packet size limit. You may want to configure this parameter if the MiNT backhaul network requires or recommends smaller packet sizes. The default value is 1500 bytes. |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-mint-policy-global-default)#mtu 1000
nx9500-6C8809(config-mint-policy-global-default)#show context
mint-policy global-default
 mtu 996
 level 2 area-id 2
nx9500-6C8809(config-mint-policy-global-default)#
```

## Related Commands

|                                 |                                                                   |
|---------------------------------|-------------------------------------------------------------------|
| <a href="#">no</a> on page 1517 | Reverts the configured MiNT MTU value to its default (1500 bytes) |
|---------------------------------|-------------------------------------------------------------------|

## router

Configures the priority for MiNT router packets (HELLO, LSP, PSNP, and EXTVLAN)

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
router packet priority <0-7>
```

## Parameters

```
router packet priority <0-7>
```

|                              |                                                                                                                                                                                                           |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| router packet priority <0-7> | Allows you to configure the priority for MiNT router packets from 0 - 7. The default is 5.<br><br><b>Note:</b> Higher the value higher is the priority. Therefore, seven (7) represents highest priority. |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
rfs4000-229D58(config-mint-policy-global-default)#router packet priority 4
rfs4000-229D58(config-mint-policy-global-default)#show context
mint-policy global-default
```



```
router packet priority 4
rfs4000-229D58(config-mint-policy-global-default)#
```

### Related Commands

|                              |                                                        |
|------------------------------|--------------------------------------------------------|
| <code>no</code> on page 1517 | Reverts the MiNT router packet priority to default (5) |
|------------------------------|--------------------------------------------------------|

### udp

Configures MiNT UDP/IP encapsulation parameters. Use this command to configure the default UDP port used for MiNT control packet encapsulation.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
udp port <2-65534>
```

### Parameters

```
udp port <2-65534>
```

|                                   |                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>port &lt;2-65534&gt;</code> | Configures default UDP port used for MiNT control packet encapsulation <ul style="list-style-type: none"><li>• <code>&lt;2-65534&gt;</code> – Enter a value from 2 - 65534. This value specifies an alternate UDP port used by MiNT control packets and must be an even number. The specified port number plus 1 is used to carry MiNT data packets. The default value is 24576.</li></ul> |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config-mint-policy-global-default)#udp port 1024
nx9500-6C8809(config-mint-policy-global-default)#show context
mint-policy global-default
 udp port 1024
 mtu 996
 level 2 area-id 2000
 sign-unknown-device
 security-level control-and-data
 rejoin-timeout 1000
nx9500-6C8809(config-mint-policy-global-default)#
```

### Related Commands

|                              |                                                  |
|------------------------------|--------------------------------------------------|
| <code>no</code> on page 1517 | Reverts MiNT UDP/IP encapsulation to its default |
|------------------------------|--------------------------------------------------|

### no

Negates a command or reverts values to their default. When used in the config MiNT policy mode, the no command resets or reverts the following global MiNT policy parameters: routing level, MTU, router packet priority, and UDP or IP encapsulation settings.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
no [level|lsp|mtu|router|udp]
no level 2 area-id
no lsp checksum
no mtu
no router packet priority
no udp port <LINE-SINK>
```

### Parameters

```
no <PARAMETERS>
```

no <PARAMETERS> The **no** command resets or reverts the following global MiNT policy parameters: routing level, MTU, router packet priority, and UDP or IP encapsulation settings.

### Examples

The following example shows the global Mint Policy parameters before the 'no' commands are executed:

```
nx9500-6C8809(config-mint-policy-global-default)#show context
mint-policy global-default
 udp port 1024
 mtu 996
 level 2 area-id 2000
 sign-unknown-device
 security-level control-and-data
 rejoin-timeout 1000
nx9500-6C8809(config-mint-policy-global-default)#
nx9500-6C8809(config-mint-policy-global-default)#no level 2 area-id
nx9500-6C8809(config-mint-policy-global-default)#no mtu
nx9500-6C8809(config-mint-policy-global-default)#no udp port
```

The following example shows the global Mint Policy parameters after the 'no' commands are executed:

```
nx9500-6C8809(config-mint-policy-global-default)#show context
mint-policy global-default
 sign-unknown-device
 security-level control-and-data
 rejoin-timeout 1000
nx9500-6C8809(config-mint-policy-global-default)#
```

# MANAGEMENT POLICY

## MANAGEMENT-POLICY

---

This chapter summarizes management policy commands in the CLI command structure.

A management policy contains configuration elements for managing a device, such as access control, SNMP, admin user credentials, and roles.

A controller (wireless controller, access point, or service platform) uses mechanisms to allow or deny device access to separate interfaces and protocols (HTTP, HTTPS, Telnet, SSH or SNMP). Management access can be enabled or disabled as required for unique policies. The management access functionality is not meant to function as an ACL (in routers or other firewalls), where administrators specify and customize specific IPs to access specific interfaces.

Controllers and service platforms can be managed using multiple interfaces (SNMP, CLI, and Web UI). By default, management access is unrestricted, allowing management access to any enabled IP interface from any host using any enabled management service.

To enhance security, administrators can apply various restrictions as needed to:

- Restrict SNMP, CLI and Web UI access to specific hosts or subnets.
- Disable un-used and insecure interfaces as required within managed access profiles. Disabling un-used management services can dramatically reduce an attack footprint and free resources on managed devices.
- Provide authentication for management users.
- Apply access restrictions and permissions to management users.

Management restrictions can be applied to meet specific policies or industry requirements requiring only certain devices or users be granted access to critical infrastructure devices. Management restrictions can also be applied to reduce the attack footprint of the device when guest services are deployed.

Access points utilize a single management access policy, so ensure all the intended administrative roles, permissions, authentication and SNMP settings are correctly set. If an access point is functioning as a virtual controller AP, these are the access settings used by adopted access points of the same model as the virtual controller AP.

It is recommended to disable un-used and insecure interfaces as required within managed access profiles. Disabling un-used management services can dramatically reduce an attack footprint and free resources on managed devices.

Use the (config) instance to configure a management policy. To navigate to the config management policy instance, use the following commands:

```
<DEVICE> (config)#management-policy <POLICY-NAME>
```

To commit a management-policy, at least one admin user account must always be present in the management-policy:

```
<DEVICE>(config-management-policy-<POLICY-NAME>)#user admin password 0 test role superuser
access all
<DEVICE>(config-management-policy-<POLICY-NAME>)#
nx9500-6C8809(config-management-policy-test)#?
Management Mode commands:
 aaa-login Set authentication for logins
 allowed-locations Add allowed locations
 banner Define a login banner
 ftp Enable FTP server
 http Hyper Text Terminal Protocol (HTTP)
 https Secure HTTP
 idle-session-timeout Configure idle timeout for a configuration session
 (GUI or CLI)
 ipv6 IPv6 Protocol
 no Negate a command or set its defaults
 passwd-retry Lockout user if too many consecutive login failures
 privilege-mode-password Set the password for entering CLI privilege mode
 rest-server Enable rest server for device on-boarding
 functionality
 restrict-access Restrict management access to the device
 snmp-server SNMP
 ssh Enable ssh
 t5 T5 configuration
 telnet Enable telnet
 user Add a user account

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-management-policy-test)#
```

## management-policy-commands

The following table summarizes management policy configuration mode commands:

**Table 47: Management-Policy Config Mode Commands**

| Command                                        | Description                                                                                                            |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| <a href="#">aaa-login</a>                      | Configures login authentication settings                                                                               |
| <a href="#">allowed-locations</a> on page 1523 | Configures a user-role based access control to RF Domains and locations with respect to the NSight UI (user interface) |
| <a href="#">banner</a>                         | Configures the MOTD (message of the day) text                                                                          |
| <a href="#">ftp</a>                            | Enables FTP on this management policy                                                                                  |
| <a href="#">http</a>                           | Enables HTTP on this management policy                                                                                 |
| <a href="#">https</a>                          | Enables HTTPS on this management policy                                                                                |

**Table 47: Management-Policy  
Config Mode Commands  
(continued)**

| Command                                                   | Description                                                                                                                                       |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>idle-session-timeout</code>                         | Sets the interval after which an idle session is terminated                                                                                       |
| <code>ipv6 (management-policy)</code> on page 1529        | Restricts management access to specified hosts and/or subnets based on their IPv6 addresses and prefixes respectively                             |
| <code>no</code>                                           | Removes or resets this management policy's settings                                                                                               |
| <code>password-entry</code> on page 1530                  | Configures user-account lockout and unlock parameters                                                                                             |
| <code>privilege-mode-password</code>                      | Configures the CLI's privilege mode access password                                                                                               |
| <code>rest-server (management-policy)</code> on page 1534 | Enables the REST (Representational State Transfer) server to facilitate device on-boarding                                                        |
| <code>restrict-access</code>                              | Restricts management access to a set of hosts or subnets                                                                                          |
| <code>snmp-server</code>                                  | Sets the SNMP server settings on this management policy                                                                                           |
| <code>ssh</code>                                          | Enables SSH on this management policy                                                                                                             |
| <code>t5 (management-policy)</code> on page 1542          | Configures SNMP server settings for T5 devices on this management policy. This command is available only RFS 4000, NX 95XX and NX 96XX platforms. |
| <code>telnet</code>                                       | Enables Telnet on this management policy                                                                                                          |
| <code>user</code>                                         | Creates a new user account                                                                                                                        |
| <code>service</code>                                      | Invokes service commands to troubleshoot or debug (config-if) instance configurations                                                             |



**Note**

For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see [COMMON COMMANDS](#) on page 640.



**Note**

The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore ( \_ ) character. In other words, the name of a device cannot contain an underscore.

*aaa-login*

Configures AAA (Authentication, Authorization and Accounting) modes used with this management policy

**Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
aaa-login [local|radius|tacacs]
aaa-login local
aaa-login radius [external|fallback|policy]
aaa-login radius [external|fallback|policy <AAA-POLICY-NAME>]
aaa-login tacacs [accounting|authentication|authorization|fallback|policy <AAA-TACACS-
POLICY-NAME>]
```

## Parameters

```
aaa-login local
```

|       |                                                                                                                                |
|-------|--------------------------------------------------------------------------------------------------------------------------------|
| local | Sets local as the preferred authentication mode. Local authentication uses the local username database to authenticate a user. |
|-------|--------------------------------------------------------------------------------------------------------------------------------|

```
aaa-login radius [external|fallback|policy <AAA-POLICY-NAME>]
```

|                          |                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| radius                   | Configures the RADIUS server parameters<br><br><b>Note:</b> If local authentication is disabled, use this command to specify if the RADIUS server used is external, fallback, or specified by a AAA policy.                                                                                                                                                                          |
| external                 | Configures external RADIUS server as the preferred authentication server                                                                                                                                                                                                                                                                                                             |
| fallback                 | Configures RADIUS server authentication as the primary authentication mode. When RADIUS server authentication fails, the system uses local authentication. This command configures local authentication as a backup mode.                                                                                                                                                            |
| policy <AAA-POLICY-NAME> | Associates a specified AAA policy with this management policy. The AAA policy determines if a client is granted access to the network. <ul style="list-style-type: none"><li>• &lt;AAA-POLICY-NAME&gt; - Specify the AAA policy name (should be existing and configured).</li></ul><br><b>Note:</b> For more information on configuring AAA policy, see <a href="#">AAA-POLICY</a> . |

```
aaa-login tacacs [accounting|authentication|authorization|fallback|policy <AAA-TACACS-
POLICY-NAME>]
```

|                                 |                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| tacacs                          | Configures TACACS (Terminal Access Control Access-Control System) server parameters                                                                                                                                                                                                                                                        |
| accounting                      | Configures TACACS accounting                                                                                                                                                                                                                                                                                                               |
| authentication                  | Configures TACACS authentication                                                                                                                                                                                                                                                                                                           |
| authorization                   | Configures TACACS authorization                                                                                                                                                                                                                                                                                                            |
| fallback                        | Configures TACACS as the primary authentication mode. When TACACS authentication fails, the system uses local authentication. This command configures local authentication as a backup mode.                                                                                                                                               |
| policy <AAA-TACACS-POLICY-NAME> | Associates a specified AAA TACACS policy with this management policy <ul style="list-style-type: none"><li>• &lt;AAA-TACACS-POLICY-NAME&gt; - Specify the TACACS policy name (should be existing and configured).</li></ul><br><b>Note:</b> For more information on configuring AAA TACACS policy, see <a href="#">AAA-TACACS-POLICY</a> . |

## Usage Guidelines

Use AAA login to determine whether management user authentication must be performed against a local user database or an external RADIUS server.

## Examples

```
rfs4000-6DB5D4(config-management-policy-test)#aaa-login radius policy test
rfs4000-6DB5D4(config-management-policy-test)#show context
management-policy test
 http server
 no ssh
 aaa-login radius policy test
rfs4000-6DB5D4(config-management-policy-test)#
```

## Related Commands

|                 |                                           |
|-----------------|-------------------------------------------|
| <code>no</code> | Removes the TACACS server policy settings |
|-----------------|-------------------------------------------|

### *allowed-locations*

Configures a user-role based access control to RF Domains and locations with respect to the NSight UI (user interface). When configured, this access control is enforced only on the NSight UI. The WiNG and NSight applications may have the same users with different permissions defined in each application. Various user roles are supported in WiNG (superuser, system-admin, network-admin, security-admin, device-provisioning-admin, helpdesk and monitor). With NSight, users logging into the NSight UI should also have an access control restriction based on the role they are assigned. For example, a WiNG user with helpdesk privileges should have access to only the site (RF Domain) in which the helpdesk is situated, and the location tree should contain only one RF Domain. Similarly, when a user responsible for a set of sites logs in NSight, their location tree needs to contain the RF Domains for which they are responsible.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
allowed-locations <WORD> locations [NONE|ALL|<LIST-OF-LOCATIONS>]
```

### Parameters

```
allowed-locations <WORD> locations [NONE|ALL|<LIST-OF-LOCATIONS>]
```

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| allowed-locations <WORD>                 | Configures a location tag and associates a list locations with the tag <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Provide a location tag not exceeding 32 characters in length</li> </ul>                                                                                                                                                                                                                                                                               |
| locations [NONE ALL] <LIST-OF-LOCATIONS> | Associates locations with the above created location tag <ul style="list-style-type: none"> <li>• NONE – When specified, states that none of the locations are to be allowed access.</li> <li>• ALL – When specified, states that all the locations are to be allowed access.</li> <li>• &lt;LIST-OF-LOCATIONS&gt; – Specifies a list of locations or individual RF Domains. When specified, states that the specified list of locations or RF Domain are allowed access.</li> </ul> |

### Example

```

nx9500-6C8809(config-management-policy-test)#allowed-locations Ecospace locations TechPubs
ALL
nx9500-6C8809(config-management-policy-test)#allowed-locations TEST locations NONE
nx9500-6C8809(config-management-policy-test)#show context
management-policy test
 no telnet
 no http server
 https server
 ssh
 allowed-location TEST locations NONE
 allowed-location Ecospace locations TechPubs ALL
nx9500-6C8809(config-management-policy-test)#

```

### Related Commands

|    |                                             |
|----|---------------------------------------------|
| no | Removes the allowed-locations configuration |
|----|---------------------------------------------|

### banner

Configures the MOTD (message of the day) text. This text is displayed at login to clients connecting through Telnet or SSH.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
banner motd <LINE>
```

### Parameters

```
banner motd <LINE>
```

|             |                                                                                                                                                                        |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| motd <LINE> | Sets the motd banner <ul style="list-style-type: none"> <li>• &lt;LINE&gt; – Enter the message string. The message string should not exceed 255 characters.</li> </ul> |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



## Examples

```
rfs4000-6DB5D4(config-management-policy-test)#banner motd "Have a Good Day"
rfs4000-6DB5D4(config-management-policy-test)#show context
management-policy test
 http server
 no ssh
 aaa-login radius external
 aaa-login radius policy test
 banner motd "Have a Good Day"
rfs4000-6DB5D4(config-management-policy-test)#
```

## Related Commands

|                 |                         |
|-----------------|-------------------------|
| <code>no</code> | Removes the motd banner |
|-----------------|-------------------------|

## ftp

Enables FTP (File Transfer Protocol) on this management policy. FTP is the standard protocol for transferring files over a TCP/IP network. FTP requires administrators enter a valid username and password authenticated locally. FTP access is disabled by default.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
ftp {password/rootdir/username}
ftp {password [1 <ENCRYPTED-PASSWORD>|<PASSWORD>]}
ftp {rootdir <DIR>}
ftp {username <USERNAME> password [1 <ENCRYPTED-PASSWORD>|<PASSWORD>] rootdir <DIR>}
```

## Parameters

```
ftp {password [1 <ENCRYPTED-PASSWORD>|<PASSWORD>]}
```

|                        |                                                                                                                                                                                                                                                                    |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ftp password           | Optional. Configures the FTP server password                                                                                                                                                                                                                       |
| 1 <ENCRYPTED-PASSWORD> | Configures an encrypted password. Use this option when copy pasting the password from another device. <ul style="list-style-type: none"><li>• &lt;ENCRYPTED-PASSWORD&gt; - Specify the password. The password should not exceed 63 characters in length.</li></ul> |
| <PASSWORD>             | Configures a clear text password                                                                                                                                                                                                                                   |

```
ftp {rootdir <DIR>}
```

|                   |                                                                                                                                                                                                         |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ftp rootdir <DIR> | Optional. Configures the root directory for FTP logins <ul style="list-style-type: none"><li>• &lt;DIR&gt; - Specify the root directory path. By default the root directory is set to flash:/</li></ul> |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
ftp {username <USERNAME> password [1 <ENCRYPTED-PASSWORD>|<PASSWORD>] rootdir <DIR>}
```

|                                              |                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ftp username <USERNAME>                      | Optional. Configures a new user account on the FTP server. The FTP user file lists users with FTP server access. <ul style="list-style-type: none"> <li>&lt;USERNAME&gt; - Specify the username. The username should not exceed 32 characters in length.</li> </ul>                                                           |
| password [1 <ENCRYPTED-PASSWORD> <PASSWORD>] | Configures an encrypted password <ul style="list-style-type: none"> <li>1 &lt;ENCRYPTED-PASSWORD&gt; - Specifies an encrypted password (use this option if copy pasting from another device). The password should not exceed 63 characters in length.</li> <li>&lt;PASSWORD&gt; - Configures a clear text password</li> </ul> |
| rootdir <DIR>                                | After specifying the password, configure the FTP root directory. <ul style="list-style-type: none"> <li>rootdir &lt;DIR&gt; - Configures the root directory for FTP logins. Specify the root directory path.</li> </ul>                                                                                                       |

### Usage Guidelines

The string size of an encrypted password (option 1, password is encrypted with a SHA1 algorithm) must be exactly 40 characters. Copy paste the encrypted password here.

### Examples

```
rfs4000-6DB5D4(config-management-policy-test)#ftp username superuser password test@123
rootdir dir
rfs4000-6DB5D4(config-management-policy-test)#show context
management-policy test
 http server
 ftp username superuser password 1
f617ca50c59fb47028f96db4baab5f3d8f03c03ab257960b0fd127c69f02cd7e rootdir dir
 no ssh
 aaa-login radius external
 aaa-login radius policy test
 banner motd "Have a Good Day"
rfs4000-6DB5D4(config-management-policy-test)#
```

### Related Commands

|           |                                                                                       |
|-----------|---------------------------------------------------------------------------------------|
| <b>no</b> | Disables FTP and its settings, such as the server password, root directory, and users |
|-----------|---------------------------------------------------------------------------------------|

### http

Enables HTTPS (Hyper Text Transport Protocol) on this management policy

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
http server
```

### Parameters

```
http server
```

`http server` Enables HTTP on this management policy. HTTP provides limited authentication and no encryption.

### Examples

```
rfs4000-6DB5D4(config-management-policy-test)#http server
rfs4000-6DB5D4(config-management-policy-test)#show context
management-policy test
 http server
 ftp username superuser password 1
f617ca50c59fb47028f96db4baab5f3d8f03c03ab257960b0fd127c69f02cd7e rootdir dir
no ssh
aaa-login radius external
aaa-login radius policy test
banner motd "Have a Good Day"
rfs4000-6DB5D4(config-management-policy-test)#
```

### Related Commands

`no` Disables HTTP on this management policy

### *https*

Enables HTTPS (Hyper Text Transport Protocol Secure) on this management policy

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
[server|sslv3|use-secure-ciphers-only]
```

### Parameters

```
[server|sslv3|use-secure-ciphers-only]
```

|                                      |                                                                                                                                                                                                                                                      |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>https server</code>            | Configures secure HTTP related parameters on this management policy                                                                                                                                                                                  |
| <code>server</code>                  | Enables HTTPS on this management policy. HTTPS provides both authentication and data encryption as opposed to just authentication. This option is enabled by default.                                                                                |
| <code>sslv3</code>                   | Enables the use of SSLv3 protocol to connect to a Web page. When enabled, SSLv2 Web authentication is disabled, and enforces the use of Web browsers supporting SSLv3, which is a more secure protocol. This option is disabled by default.          |
| <code>use-secure-ciphers-only</code> | Enables the use of TLS v1.2 ciphers to secure client-server network communications. When enabled, for HTTPS connections the TLS v1.2 protocol is used, instead of the less secure TLS v1.0 or TLS v1.1 protocols. This option is enabled by default. |

### Examples

```
rfs4000-6DB5D4(config-management-policy-test)#https server
rfs4000-6DB5D4(config-management-policy-test)#show context
management-policy test
 http server
 https server
 ftp username superuser password 1
```

```
f617ca50c59fb47028f96db4baab5f3d8f03c03ab257960b0fd127c69f02cd7e rootdir dir
no ssh
aaa-login radius external
aaa-login radius policy test
banner motd "Have a Good Day"
rfs4000-6DB5D4(config-management-policy-test)#
```

The following example shows that the 'use-secure-ciphers-only' option is enabled by default:

```
rfs4000-6DB5D4(config-management-policy-default)#show context include-factory | include
https
https server
no https sslv3
https use-secure-ciphers-only
rfs4000-6DB5D4(config-management-policy-default)#
```

### Related Commands

|                 |                                          |
|-----------------|------------------------------------------|
| <code>no</code> | Disables HTTPS on this management policy |
|-----------------|------------------------------------------|

### *idle-session-timeout*

Configures a session's idle timeout. An idle session is automatically terminated after the specified interval is exceeded.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
idle-session-timeout <1-4320>
```

### Parameters

```
idle-session-timeout <1-4320>
```

|                             |                                                                                                                                            |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;1-4320&gt;</code> | Sets the interval, in minutes, after which an idle session is timed out. Specify a value from 1 - 4320 minutes. The default is 30 minutes. |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
rfs4000-6DB5D4(config-management-policy-test)#idle-session-timeout 100
rfs4000-6DB5D4(config-management-policy-test)#show context
management-policy test
http server
https server
ftp username superuser password 1
7ccb4568cb83e54f1e402f785a78ee930a453afda152baaf7c2b79277f225872 rootdir dir
no ssh
aaa-login radius external
aaa-login radius policy test
idle-session-timeout 100
banner motd "Have a Good Day"
rfs4000-6DB5D4(config-management-policy-test)#
```

## Related Commands

|                 |                                                   |
|-----------------|---------------------------------------------------|
| <code>no</code> | Removes the configured idle session timeout value |
|-----------------|---------------------------------------------------|

### *ipv6 (management-policy)*

Restricts management access to specified hosts and/or subnets based on their IPv6 addresses and prefixes respectively

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
ipv6 restrict-access [host|ipv6-access-list|subnet]
ipv6 restrict-access host <IPv6> {log|subnet}
ipv6 restrict-access host <IPv6> {log [all|denied-only]}
ipv6 restrict-access host <IPv6> {subnet <IPv6-PREFIX> {log [all|denied-only]}}
ipv6 restrict-access ipv6-access-list <IPv6-ACCESS-LIST-NAME>
ipv6 restrict-access subnet <IPv6-PREFIX> {host|log}
ipv6 restrict-access subnet <IPv6-PREFIX> {log [all|denied-only]}
ipv6 restrict-access subnet <IPv6-PREFIX> {host <IPv6> {log [all|denied-only]}}
```

#### Parameters

```
ipv6 restrict-access host <IPv6> {log [all|denied-only]}
```

|                       |                                                                                                                                                                                                                                                             |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| host <IPv6>           | Restricts management access to a specified host, based on the host's IPv6 address <ul style="list-style-type: none"><li>• &lt;IPv6&gt; - Specify the host's IPv6 address.</li></ul>                                                                         |
| log [all denied-only] | Optional. Configures a logging policy for access requests <ul style="list-style-type: none"><li>• all - Logs all access requests, both denied and permitted</li><li>• denied-only - Logs only denied access events (when a host is denied access)</li></ul> |

```
ipv6 restrict-access host <IPv6> {subnet <IPv6-PREFIX> {log [all|denied-only]}}
```

|                       |                                                                                                                                                                                                                                                                    |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| host <IPv6>           | Restricts management access to a specified host, based on the host's IPv6 address <ul style="list-style-type: none"><li>• &lt;IPv6&gt; - Specify the host's IPv6 address.</li></ul>                                                                                |
| subnet <IPv6-PREFIX>  | Optional. Restricts access to the host on a specified IPv6 subnet <ul style="list-style-type: none"><li>• &lt;IPv6-PREFIX&gt; - Specify the subnet's IPv6 prefix in the X:X::X:X/M format.</li></ul>                                                               |
| log [all denied-only] | Optional. Configures a logging policy for access requests <ul style="list-style-type: none"><li>• all - Logs all access requests, both denied and permitted</li><li>• denied-only - Logs only denied access events (when a host/subnet is denied access)</li></ul> |

```
ipv6 restrict-access ipv6-access-list <IPv6-ACCESS-LIST-NAME>
```

|                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>ipv6-access-list &lt;IPv6-ACCESS-LIST-NAME&gt;</code> | <p>Uses an IPv6 ACL (Access Control List) to filter access requests. IPv6 ACLs filter/mark packets based on the IPv6 address from which they arrive. IPv6 hosts configure themselves automatically when connected to an IPv6 network using the ND (neighbor discovery) protocol via ICMPv6 router discovery messages. These hosts require firewall packet protection unique to IPv6 traffic, as IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. An existing IPv6 ACL can be created and used in the management policy context to permit or deny access to specific hosts and/or subnets.</p> <ul style="list-style-type: none"> <li>• <code>&lt;IPv6-ACCESS-LIST-NAME&gt;</code> - Specify the IPv6 ACL name.</li> </ul> |
|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
ipv6 restrict-access subnet <IPv6-PREFIX> {log [all|denied-only]}
```

|                                         |                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>subnet &lt;IPv6-PREFIX&gt;</code> | <p>Restricts management access to a specified IPv6 subnet</p> <ul style="list-style-type: none"> <li>• <code>&lt;IPv6-PREFIX&gt;</code> - Specify the subnet's IPv6 prefix in the X::X::X/M format.</li> </ul>                                                                                         |
| <code>log [all denied-only]</code>      | <p>Optional. Configures a logging policy for access requests</p> <ul style="list-style-type: none"> <li>• <code>all</code> - Logs all access requests, both denied and permitted</li> <li>• <code>denied-only</code> - Logs only denied access events (when a host/subnet is denied access)</li> </ul> |

```
ipv6 restrict-access subnet <IPv6-PREFIX> {host <IPv6> {log [all|denied-only]}}
```

|                                         |                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>subnet &lt;IPv6-PREFIX&gt;</code> | <p>Restricts management access to a specified IPv6 subnet</p> <ul style="list-style-type: none"> <li>• <code>&lt;IPv6-PREFIX&gt;</code> - Specify the subnet's IPv6 prefix in the X::X::X/M format.</li> </ul>                                                                                         |
| <code>host &lt;IPv6&gt;</code>          | <p>Optional. Restricts management access to a specific host within the specified subnet</p> <ul style="list-style-type: none"> <li>• <code>&lt;IPv6&gt;</code> - Specify the host's IPv6 address.</li> </ul>                                                                                           |
| <code>log [all denied-only]</code>      | <p>Optional. Configures a logging policy for access requests</p> <ul style="list-style-type: none"> <li>• <code>all</code> - Logs all access requests, both denied and permitted</li> <li>• <code>denied-only</code> - Logs only denied access events (when a host/subnet is denied access)</li> </ul> |

### Example

```
rfs4000-6DB5D4(config-management-policy-test)#ipv6 restrict-access host 2001:fdbc:06cf:0011::13 subnet 2001:fdbc:06cf:0011::0/64 log all
rfs4000-6DB5D4(config-management-policy-test)#show context
management-policy test
 http server
 no ssh
 ipv6 restrict-access host 2001:fdbc:06cf:0011::13 subnet 2001:fdbc:06cf:0011::0/64 log all
rfs4000-6DB5D4(config-management-policy-test)#
```

### Related Commands

|                 |                                                |
|-----------------|------------------------------------------------|
| <code>no</code> | Removes management access restriction settings |
|-----------------|------------------------------------------------|

### *password-entry*

Configures user-account lockout and unlock parameters. Use this option to configure the maximum number of consecutive, failed login attempts allowed before an account is locked out, and the duration of lockout.

## Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
passwd-entry role [device-provisioning-admin|helpdesk|monitor|network-admin|security-admin|superuser|system-admin|vendor-admin|web-user-admin] max-fail <1-100> lockout-time <0-600>
```

## Parameters

```
passwd-entry role [device-provisioning-admin|helpdesk|monitor|network-admin|security-admin|superuser|system-admin|vendor-admin|web-user-admin] max-fail <1-100> lockout-time <0-600>
```

|                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>passwd-entry role [device-provisioning-admin helpdesk monitor network-admin security-admin superuser system-admin vendor-admin web-user-admin] max-fail &lt;1-100&gt; lockout-time &lt;0-600&gt;</pre> | <p>Configures user-role based account lockout criteria</p> <ul style="list-style-type: none"><li>• role - Select the user-role. The options are:<ul style="list-style-type: none"><li>• device-provisioning-admin</li><li>• helpdesk</li><li>• monitor</li><li>• network-admin</li><li>• security-admin</li><li>• system-admin</li><li>• vendor-admin</li><li>• web-user-admin</li></ul></li></ul> <p>max-fail &lt;1-100&gt; - Specify the maximum number of consecutive, failed attempts allowed before an account is locked. Specify a value from 1 - 100.</p> <p>lockout-time &lt;&lt;0-600&gt;&gt; - Specify the maximum time, in minutes, for which an account remains locked. The value '0' indicates that the account is permanently locked. Specify a value from 0 - 600 minutes.</p> <p>When configured, the lockout is individually applied to each account within the specified role/roles. For example, consider the 'monitor' role having two users: 'user1' and 'user2'. The max-fail and lockout-time is set at '5' attempts and '10' minutes respectively. In this scenario, user2 makes 5 consecutive, failed login attempts, and the user2 account is locked out for 10 minutes. However, during this lockout time the user1 account remains active.</p> <p><b>Note:</b> In the event-system-policy context, enable 'login-lockout' and 'login-unlocked' event notification to trigger e-mail or syslog notification to users on occurrence of the login-lockout and login-unlock events. For more information, see <a href="#">event</a> on page 378.</p> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Example

```
rfs4000-6DB5D4(config-management-policy-default)#passwd-retry role monitor max-fail 5
lockout-time 10
rfs4000-6DB5D4(config-management-policy-default)#show con
management-policy default
no telnet
no http server
https server
ssh
user admin password 1 979cfb9288837ee26d74d07b5ea328fd0e9a2b55cf5104649c2b496cc94e7003
```

```

role superuser access all
passwd-retry role monitor max-fail 2 lockout-time 5
snmp-server community 0 private rw
snmp-server community 0 public ro
snmp-server user snmptrap v3 encrypted des auth md5 0 admin123
snmp-server user snmpmanager v3 encrypted des auth md5 0 admin123
rfs4000-6DB5D4(config-management-policy-default)#

```

## Related Commands

|                 |                                                                        |
|-----------------|------------------------------------------------------------------------|
| <code>no</code> | Removes the user-account lockout and unlock parameters configured here |
|-----------------|------------------------------------------------------------------------|

### *privilege-mode-password*

Configures the CLI's privilege mode access password. Use this option to strengthen security by enforcing a second level authentication to access the privilege configuration mode.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
privilege-mode-password <PASSWORD/HASHED-STRING-ALIAS-NAME>
```

#### Parameters

```
privilege-mode-password <PASSWORD/HASHED-STRING-ALIAS-NAME>
```

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| privilege-mode-password             | <p>Configures the password required to enter the privilege configuration mode. When configured, users are prompted to provide the password when enabling the privilege configuration mode.</p> <ul style="list-style-type: none"> <li>•</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <PASSWORD/HASHED-STRING-ALIAS-NAME> | <p>&lt;PASSWORD/HASHED-STRING-ALIAS-NAME&gt; - Enter the password as a clear text, or provide a hashed-string alias. Enter the password as a clear text, or provide a hashed-string alias. If using a hashed-string alias, ensure that the alias is existing and configured.</p> <p><b>Note:</b> The clear text password is saved and displayed as a hashed string. Hashing is a means of establishing the integrity of transmitted messages. Before transmission, a hash of the message is generated, encrypted and sent along with the message. At the receiving end, the message and the hash are both decrypted, and another hash is generated from the received message. The two hashes are compared. If both are identical the message is considered to have been transmitted intact.</p> <p><b>Note:</b> For more information on configuring a hashed-string alias, see alias.</p> |



## Examples

The following example shows the privilege mode password being configured as a hashed string:

```
rfs4000-6DB5D4(config-management-policy-test)#privilege-mode-password 1
2e9f038ac2ed27f919ed5a4dceb3d30e32f356f2ceff6fbf26a153d0339c734f
rfs4000-6DB5D4(config-management-policy-test)#show context
management-policy test
 http server
 no ssh
 privilege-mode-password 1 2e9f038ac2ed27f919ed5a4dceb3d30e32f356f2ceff6fbf26a153d0339c734f
rfs4000-6DB5D4(config-management-policy-test)#
```

### Example: Configuring privilege mode password using a hashed-string alias.

Follow the steps below to configure a hashed-string alias and use it as a privilege mode password:

- 1 In the global-configuration context, create a hashed-string alias.

```
nx9500-6C8809(config)#alias hashed-string $PriMode Test12345
nx9500-6C8809(config)#show context | include alias
alias vlan $BLR-01 1
alias string $IN-Blr-EcoSpace-Floor-4 IBEF4
alias encrypted-string $READ 0 public
alias encrypted-string $WRITE 0 private
alias hashed-string $PriMode 1
faffdde27cb49ad634ea20df4f7c8ef2685894d10ffcblb2efba054112ecfc75
nx9500-6C8809(config)#
```

- 2 In the management-policy context, configure the hashed-string alias created in step 1 as the privilege mode password.

```
nx9500-6C8809(config-management-policy-default)#privilege-mode-password $PrivMode
nx9500-6C8809(config-management-policy-default)#show context
management-policy default
https server
rest-server
ssh
user admin password 1 ad4d8797f007444ccdda3788b9ee0e8b46f3facb4308e045239eb7771e127ed5
role superuser access all
snmp-server community 0 $WRITE rw
snmp-server community 0 $READ ro
snmp-server user snmptrap v3 encrypted des auth md5 2 yqr96yyVzmD4ZbU2I7Eh/
QAAAajWNKa4KXF95pruUCSnhOiT
snmp-server user snmpmanager v3 encrypted des auth md5 2 NOF8+2+AY2r4ZbU2I7Eh/
QAAAagc0l8ahJYo3AjHo9wXzYGo
t5 snmp-server community public ro 192.168.0.1
t5 snmp-server community private rw 192.168.0.1
privilege-mode-password $PriMode
nx9500-6C8809(config-management-policy-default)#
```

- 3 Confirm, if the privilege mode is password protected.

```
nx9500-6C8809 login: admin
Password:
Feb 07 14:40:47 2017: %AUTH-6-INFO: login[28768]: user 'admin' on 'ttyS0' from
'Console' logged in
Feb 07 14:40:47 2017: nx9500-6C8809 : %SYSTEM-5-LOGIN: Successfully logged in user
'admin' with privilege 'superuser' from 'ttyS0'
nx9500-6C8809>en
Password:
```

## Related Commands

|                                                                     |
|---------------------------------------------------------------------|
| <b>no</b> Removes the configured CLI privilege mode access password |
|---------------------------------------------------------------------|

## *rest-server (management-policy)*

Enables the REST (Representational State Transfer) server. When enabled, the REST server allows vendor users access to the online device registration portal. All requests and responses to and from the on-boarding portal are handled by the REST server through restful API (Application Programming Interface) transactions. The REST server serves the Web pages used to associate a device's MAC address with a specific vendor group.

Each vendor has a 'vendor-admin' user who is assigned a unique, username/password credential for RADIUS server validation. Successfully validated vendor-admins can access the online device registration portal to on-board devices. For more information on vendor-admin user configuration, see [user \(management-policy\)](#) on page 1544.

The REST server is enabled by default.

### **Supported in the following platforms:**

- Service Platforms — NX 95XX, NX 96XX, VX 9000

### **Syntax**

```
rest-server
```

### **Parameters**

None

### **Example**

```
nx9500-6C8809(config-management-policy-testMNGTPolicy)#show context
management-policy testMNGTPolicy
 no telnet
 no http server
 https server
 rest-server
 ssh
nx9500-6C8809(config-management-policy-testMNGTPolicy)#
nx9500-6C8809(config-management-policy-testMNTPolicy)#no rest-server
nx9500-6C8809(config-management-policy-testMNGTPolicy)#show context
management-policy testMNGTPolicy
 no telnet
 no http server
 https server
 no rest-server
 ssh
nx9500-6C8809(config-management-policy-testMNGTPolicy)#
```

### **Related Commands**

|                 |                          |
|-----------------|--------------------------|
| <code>no</code> | Disables the REST server |
|-----------------|--------------------------|

## *restrict-access*

Restricts management access to a set of hosts or subnets

Restricting remote access to a controller or service platform ensures only trusted hosts can communicate with enabled management services. This ensures only trusted hosts can perform

management tasks and provide protection from brute force attacks from hosts attempting to break into the controller or service platform managed network.

Administrators can permit management connections to be established on any IP interface on the controller or service platform (including IP interfaces used to provide captive portal guest access). Administrators can restrict management access by limiting access to a specific host (IP address), subnet, or ACL on the controller or service platform.

**Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

**Syntax**

```
restrict-access [host|ip-access-list|subnet]
restrict-access host <IP> {log|subnet}
restrict-access host <IP> {log [all|denied-only]}
restrict-access host <IP> {subnet <IP/M> {log [all|denied-only]}}
restrict-access ip-access-list <IP-ACCESS-LIST-NAME>
restrict-access subnet <IP/M> {host|log}
restrict-access subnet <IP/M> {log [all|denied-only]}
restrict-access subnet <IP/M> {host <IP> {log [all|denied-only]}}
```

**Parameters**

```
restrict-access host <IP> {log [all|denied-only]}
```

|                       |                                                                                                                                                                                                                                                                                                              |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| host <IP>             | Restricts management access to a specified host. Filters access requests based on a host's IP address <ul style="list-style-type: none"> <li>• &lt;IP&gt; - Specify the host's IPv4 address.</li> </ul>                                                                                                      |
| log [all denied-only] | Optional. Configures a logging policy for access requests. <ul style="list-style-type: none"> <li>• all - Logs all access requests, both denied and permitted</li> <li>• denied-only - Logs only denied access (when an access request is received from a host denied access, a record is logged)</li> </ul> |

```
restrict-access host <IP> {subnet <IP/M> {log [all|denied-only]}}
```

|                       |                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| host <IP>             | Restricts management access to a specified host. Filters access requests based on a host's IP address <ul style="list-style-type: none"> <li>• &lt;IP&gt; - Specify the host's IPv4 address.</li> </ul>                                                                                                                                                      |
| subnet <IP/M>         | Optional. Restricts access on a specified subnet <ul style="list-style-type: none"> <li>• &lt;IP/M&gt; - Sets the subnet in the A.B.C.D/M format</li> </ul>                                                                                                                                                                                                  |
| log [all denied-only] | Optional. Configures a logging policy for access requests. Sets the log type generated for access requests <ul style="list-style-type: none"> <li>• all - Logs all access requests, both denied and permitted</li> <li>• denied-only - Logs only denied access (when an access request is received from a host denied access, a record is logged)</li> </ul> |

```
restrict-access ip-access-list <IP-ACCESS-LIST-NAME>
```

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip-access-list         | Uses an IPv4 access list to filter access requests<br>IPv4 ACLs filter/mark packets based on the IPv4 address from which they arrive. IP and non-IP traffic, on the same layer 2 interface, can be filtered by applying an IPv4 ACL. Each IPv4 ACL contains a set of deny and/or permit rules. Each rule is specific to source and destination IPv4 addresses and the unique rules and precedence definitions assigned. When the network traffic matches the criteria specified in one of these rules, the action defined in that rule is used to determine whether the traffic is allowed or denied. |
| <IP-ACCESS-LIST- NAME> | Specify the IPv4 ACL name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

```
restrict-access subnet <IP/M> {<IP/M>/log [all|denied-only]}
```

|                       |                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| subnet <IP/M>         | Restricts management access to a specified subnet <ul style="list-style-type: none"> <li>• &lt;IP/M&gt; - Specify the subnet in the A.B.C.D/M format</li> </ul>                                                                                                                                                                                                   |
| log [all denied-only] | Optional. Configures a logging policy for access requests. Sets the log type generated for access requests <ul style="list-style-type: none"> <li>• all - Logs all access requests, both denied and permitted</li> <li>• denied-only - Logs only denied access events (when access request received from a host within the specified subnet is denied)</li> </ul> |

```
restrict-access subnet <IP/M> {host <IP> {log [all|denied-only]}}
```

|                       |                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| subnet <IP/M>         | Restricts management access to a specified subnet <ul style="list-style-type: none"> <li>• &lt;IP/M&gt; - Specify the subnet in the A.B.C.D/M format</li> </ul>                                                                                                                                                                                                   |
| host <IP>             | Uses the host IP address as a second filter <ul style="list-style-type: none"> <li>• &lt;IP&gt; - Specify the host's IPv4 address.</li> </ul>                                                                                                                                                                                                                     |
| log [all denied-only] | Optional. Configures a logging policy for access requests. Sets the log type generated for access requests <ul style="list-style-type: none"> <li>• all - Logs all access requests, both denied and permitted</li> <li>• denied-only - Logs only denied access events (when access request received from a host within the specified subnet is denied)</li> </ul> |

## Examples

```
rfs4000-6DB5D4(config-management-policy-test)#restrict-access host 172.16.10.4 log denied-only
rfs4000-6DB5D4(config-management-policy-test)#show context
management-policy test
no http server
https server
ftp username superuser password 1
626b4033263d6d2ae4e79c48cdfcccb60fd4c77a8da9e365060597a6d6570ec2 rootdir dir
no ssh
aaa-login radius external
aaa-login radius policy test
idle-session-timeout 0
restrict-access host 172.16.10.4 log denied-only
rfs4000-6DB5D4(config-management-policy-test)#
```

## Related Commands

|    |                                    |
|----|------------------------------------|
| no | Removes device access restrictions |
|----|------------------------------------|

## snmp-server

Enables the SNMP (Simple Network Management Protocol) engine settings. SNMP is an application layer protocol that facilitates the exchange of management information between the controller and a managed device. SNMP enabled devices listen on port 162 (by default) for SNMP packets from the controller's management server. SNMP uses read-only and read-write community strings as an authentication mechanism to monitor and configure supported devices. The read-only community string gathers statistics and configuration parameters from a supported wireless device. The read-write community string is used by a management server to set device parameters. SNMP is generally used to monitor a system's performance and other parameters.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
snmp-server [community|enable|display-vlan-info-per-radio|host|manager|max-pending-requests|request-timeout|suppress-security-configuration-level|throttle|user]
snmp-server community [0 <WORD>|2 <WORD>|<WORD>] [ro|rw] {ip-snmp-access-list <IP-SNMP-ACL-NAME>}
snmp-server enable traps
snmp-server host <IP> [v1|v2c|v3] {<1-65535>}
snmp-server manager [all|v1|v2|v3]
snmp-server [max-pending-requests {<64-1024>}|request-timeout {<2-720>}]
snmp-server [display-vlan-info-per-radio|throttle <1-100>|suppress-security-configuration-level [0|1]]
snmp-server user [snmpmanager|snmpoperator|snmptrap]
snmp-server user [snmpmanager|snmpoperator|snmptrap] v3 [auth|encrypted]
snmp-server user [snmpmanager|snmpoperator|snmptrap] v3 auth md5 [0 <PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>]
snmp-server user [snmpmanager|snmpoperator|snmptrap] v3 encrypted [auth md5|des auth md5] [0 <PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>]
```

### Parameters

```
snmp-server community [0 <WORD>|2 <WORD>|<WORD>] [ro|rw] {ip-snmp-access-list <IP-SNMP-ACL-NAME>}
```

|                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| community [0<br><WORD>] 2<br><WORD> <br><WORD>] | <p>Sets the community string and associated access privileges. Define a public or private community designation. By default, SNMPv2 community strings on most devices are set to public for the read-only community string, and private for the read-write community string.</p> <ul style="list-style-type: none"> <li>• 0 &lt;WORD&gt; – Sets a clear text SNMP community string</li> <li>• 2 &lt;WORD&gt; – Sets an encrypted SNMP community string</li> <li>• &lt;WORD&gt; – Sets the SNMP community string</li> </ul> |
| [ro rw]                                         | <p>After configuring the SNMP community string, set the access permission for each community string used by devices to retrieve or modify information. Available options include</p> <ul style="list-style-type: none"> <li>• ro – Assigns read-only access to the specified SNMP community (allows a remote device to retrieve information)</li> <li>• rw – Assigns read and write access to the specified SNMP community (allows a remote device to modify settings)</li> </ul>                                          |
| ip-snmp-access-<br>list <IP-SNMP-ACL-<br>NAME>  | <p>Optional. Associates an IP SNMP access list (should be existing and configured). The IP SNMP ACL sets the SNMP management station's IP address. SNMP trap information is received at this address.</p>                                                                                                                                                                                                                                                                                                                  |

#### snmp-server enable traps

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| enable traps | <p>Enables trap generation (using the trap receiver configuration defined). This feature is disabled by default. Enabling this feature ensures the dispatch of SNMP notifications to all hosts.</p> <p>In a managed network, the controller uses SNMP trap receivers to notify faults. SNMP traps are unsolicited notifications triggered by thresholds (or actions) on devices and are therefore an important fault management tool.</p> <p>A SNMP trap receiver is the destination of SNMP messages (external to the controller). A trap is like a Syslog message, just over another protocol (SNMP). A trap is generated when a device consolidates event information and transmits the information to an external repository. The trap contains several standard items, such as the SNMP version, community, etc.</p> <p>SNMP trap notifications exist for most controller operations, but not all are necessary for day-to-day operation.</p> |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### snmp-server host <IP> [v1|v2c|v3] {<1-65535>}

|           |                                                                                                                                                                                                                                                                                                                                |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| host <IP> | <p>Configures a host's IP address. This is the external server resource dedicated to receiving SNMP traps on behalf of the controller.</p>                                                                                                                                                                                     |
| [v2c v3]  | <p>Configures the SNMP version used to send the traps</p> <ul style="list-style-type: none"> <li>• v1 – Uses SNMP version 1. This option is disabled by default.</li> <li>• v2c – Uses SNMP version 2c. This option is disabled by default.</li> <li>• v3 – Uses SNMP version 3. This option is enabled by default.</li> </ul> |
| <1-65535> | <p>Optional. Configures the virtual port of the server resource dedicated to receiving SNMP traps</p> <ul style="list-style-type: none"> <li>• &lt;1-65535&gt; – Optional. Specify a value from 1 - 65535. The default port is 162.</li> </ul>                                                                                 |

#### snmp-server manager [a11|v1|v2|v3]

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| manager [all v1 v2 v3] | <p>Enables SNMP manager and specifies the SNMP version</p> <ul style="list-style-type: none"> <li>all – Enables SNMP manager version v1, v2 and v3</li> <li>v1 – Enables SNMP manager version v1 only. SNMPv1 uses a simple password (“community string”). Data is unencrypted (clear text). Consequently it provides limited security, and should be used only inside LANs behind firewalls, not in WANs.</li> <li>v2 – Enables SNMP manager version v2 only. SNMPv2 provides device management using a hierarchical set of variables. SNMPv2 uses Get, GetNext, and Set operations for data management. SNMPv2 is enabled by default.</li> <li>v3 – Enables SNMP manager version v3 only. SNMPv3 adds security and remote configuration capabilities to previous versions. The SNMPv3 architecture introduces the USM (User-based Security Model) for message security and the VACM (View-based Access Control Model) for access control. The architecture supports the concurrent use of different security, access control and message processing techniques. SNMPv3 is enabled by default.</li> </ul> |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
snmp-server[max-pending-requests {<64-1024>}|request-timeout {<2-720>}]
```

|                                  |                                                                                                                                                                                                                                                    |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| max-pending-requests {<64-1024>} | <p>Sets the maximum number of requests that can be pending at any given time</p> <ul style="list-style-type: none"> <li>&lt;64-1024&gt; – Optional. Specify a value from 64 - 1024. The default is 128.</li> </ul>                                 |
| request-timeout {<2-720>}        | <p>Sets the interval, in seconds, after which an error message is returned for a pending request</p> <ul style="list-style-type: none"> <li>&lt;2-720&gt; – Optional. Specify a value from 2 - 720 seconds. The default is 240 seconds.</li> </ul> |

```
snmp-server [display-vlan-info-per-radio|throttle <1-100>|suppress-security-configuration-level [0|1]]
```

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| display-vlan-info-per-radio                 | Enables the display of the VLAN ID along with the radio interface ID                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| throttle <1-100>                            | Sets CPU usage for SNMP activities. Use this command to set the CPU usage from 1 - 100.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| suppress-security-configuration-level [0 1] | <p>Sets the level of suppression of SNMP security configuration information</p> <ul style="list-style-type: none"> <li>0 – If this option is selected, an empty string is returned for the SNMP request for security configuration information. Security configuration information consists of: <ul style="list-style-type: none"> <li>Passwords</li> <li>Keys</li> <li>Shared secrets</li> </ul> <p>The default setting is 0.</p> </li> <li>1 – Suppresses the display of the policy, IP ACL, passwords, keys and shared secrets. If this option is selected, in addition to suppression from ‘Level 0’, an empty string is returned for a SNMP request on following items: <ul style="list-style-type: none"> <li>Management policies</li> <li>IP ACL</li> <li>Tables containing user names and community strings</li> </ul> </li> </ul> |

```
snmp-server user [snmpmanager|snmpoperator|snmptrap] v3 auth md5 [0 <PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>]
```

|                                                    |                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| user [snmpmanager snmpoperator  snmptrap]          | <p>Defines user access to the SNMP engine</p> <ul style="list-style-type: none"> <li>• snmpmanager – Sets user as a SNMP manager</li> <li>• snmpoperator – Sets user as a SNMP operator</li> <li>• snmptrap – Sets user as a SNMP trap user</li> </ul>                                                                           |
| v3 auth md5                                        | <p>Uses SNMP version 3 as the security model</p> <ul style="list-style-type: none"> <li>• auth – Uses an authentication protocol <ul style="list-style-type: none"> <li>• md5 – Uses HMAC-MD5 algorithm for authentication</li> </ul> </li> </ul>                                                                                |
| [0 <PASSWORD>  2 <ENCRYPTED-PASSWORD>  <PASSWORD>] | <p>Configures password using one of the following options:</p> <ul style="list-style-type: none"> <li>• 0 &lt;PASSWORD&gt; – Configures clear text password</li> <li>• 2 &lt;PASSWORD&gt; – Configures encrypted password</li> <li>• &lt;PASSWORD&gt; – Specifies a password for authentication and privacy protocols</li> </ul> |

```
snmp-server user [snmpmanager|snmpoperator|snmptrap] v3 encrypted
[auth md5|des auth md5] [0 <PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>]
```

|                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| user [snmpmanager snmpoperator  snmptrap]          | <p>Defines user access to the SNMP engine</p> <ul style="list-style-type: none"> <li>• snmpmanager – Sets user as a SNMP manager</li> <li>• snmpoperator – Sets user as a SNMP operator</li> <li>• snmptrap – Sets user as a SNMP trap user</li> </ul>                                                                                                                                                               |
| v3 encrypted                                       | <p>Uses SNMP version 3 as the security model</p> <ul style="list-style-type: none"> <li>• encrypted – Uses encrypted privacy protocol</li> </ul>                                                                                                                                                                                                                                                                     |
| auth md5                                           | <p>Uses authentication protocol</p> <ul style="list-style-type: none"> <li>• auth – Sets authentication parameters <ul style="list-style-type: none"> <li>• md5 – Uses HMAC-MD5 algorithm for authentication</li> </ul> </li> </ul>                                                                                                                                                                                  |
| des auth md5                                       | <p>Uses privacy protocol for user privacy</p> <ul style="list-style-type: none"> <li>• des – Uses CBC-DES for privacy</li> </ul> <p>After specifying the privacy protocol, specify the authentication mode.</p> <ul style="list-style-type: none"> <li>• auth – Sets user authentication parameters <ul style="list-style-type: none"> <li>• md5 – Uses HMAC-MD5 algorithm for authentication</li> </ul> </li> </ul> |
| [0 <PASSWORD>  2 <ENCRYPTED-PASSWORD>  <PASSWORD>] | <p>The following are common to both the auth and des parameters:<br/>Configures password using one of the following options:</p> <ul style="list-style-type: none"> <li>• 0 &lt;PASSWORD&gt; – Configures a clear text password</li> <li>• 2 &lt;PASSWORD&gt; – Configures an encrypted password</li> <li>• &lt;PASSWORD&gt; – Specifies a password for authentication and privacy protocols</li> </ul>              |

## Examples

```
rfs4000-6DB5D4(config-management-policy-test)#snmp-server community snmpl ro
rfs4000-6DB5D4(config-management-policy-test)#snmp-server host 172.16.10.23 v3 162
rfs4000-6DB5D4(config-management-policy-test)#snmp-server user snmpmanager v3 auth md5
test@123
rfs4000-6DB5D4(config-management-policy-test)#show context
management-policy test
no http server
https server
```



```

ftp username superuser password 1
f617ca50c59fb47028f96db4baab5f3d8f03c03ab257960b0fd127c69f02cd7e rootdir dir
no ssh
snmp-server community snmp1 ro
snmp-server user snmpmanager v3 encrypted des auth md5 0 test@123
snmp-server host 172.16.10.23 v3 162
aaa-login radius external
aaa-login radius policy test
idle-session-timeout 0
restrict-access host 172.16.10.2 log all
rfs4000-6DB5D4(config-management-policy-test)#

```

## Related Commands

|    |                                             |
|----|---------------------------------------------|
| no | Disables or resets the SNMP server settings |
|----|---------------------------------------------|

## ssh

Enables SSH (Secure Shell) for this management policy

SSH, like Telnet, provides a command line interface to a remote host. SSH transmissions are encrypted and authenticated, increasing the security of transmission. SSH access is enabled by default.



### Note

If the RADIUS server is not reachable, SSH management access to the controller or access point may be denied. RADIUS support is available locally on controllers and access points, with the exception of the AP 6522 model, which requires an external RADIUS resource.

## Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
ssh {login-grace-time <60-300>|port <1-65535>}
```

## Parameters

```
ssh {login-grace-time <60-300>|port <1-65535>}
```

|                              |                                                                                                                                                                                                                                                                        |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ssh                          | Enables SSH communication between client and server                                                                                                                                                                                                                    |
| login-grace-time<br><60-300> | Optional. Configures the login grace time. This is the interval, in seconds, after which an unsuccessful login is disconnected. <ul style="list-style-type: none"> <li>• &lt;60-300&gt; – Specify a value from 60 - 300 seconds. The default is 60 seconds.</li> </ul> |
| port <1-65535>               | Optional. Configures the SSH port. This is the port used for SSH connections. <ul style="list-style-type: none"> <li>• &lt;1-65535&gt; – Specify a value from 1 - 165535. The default port is 22.</li> </ul>                                                           |

## Examples

```

rfs4000-6DB5D4(config-management-policy-test)#ssh port 162
rfs4000-6DB5D4(config-management-policy-test)#show context
management-policy test

```

```

no http server
https server
ftp username superuser password 1
626b4033263d6d2ae4e79c48cdfccb60fd4c77a8da9e365060597a6d6570ec2 rootdir dir
ssh port 162
snmp-server community snmp1 ro
snmp-server user snmpmanager v3 encrypted des auth md5 0 test123
snmp-server host 172.16.10.23 v3 162
aaa-login radius external
aaa-login radius policy test
idle-session-timeout 0
restrict-access host 172.16.10.2 log all
rfs4000-6DB5D4(config-management-policy-test)#

```

## Related Commands

|                 |                                                     |
|-----------------|-----------------------------------------------------|
| <code>no</code> | Resets SSH access port to factory default (port 22) |
|-----------------|-----------------------------------------------------|

### *t5 (management-policy)*

Configures SNMP server settings for T5 devices on this management policy

A T5 controller is an external device that can be adopted and managed by a WiNG controller. When enabled as a supported external device, a T5 controller can provide data to WiNG to assist in its management within a WiNG supported subnet.

This command enables SNMP to communicate with T5 devices within the network. SNMP facilitates the exchange of management information between the controller or service platform and the T5 device. For more information, see [snmp-server](#) on page 1537.

### Supported in the following platforms:

- Wireless Controllers — RFS 4000, RFS 6000
- Service Platforms — NX 95XX, NX 96XX

### Syntax

```

t5 snmp-server [community|contact|enable|host|location]
t5 snmp-server community <COMMUNITY-NAME> [ro|rw] <SNMP-STATION-IP>
t5 snmp-server contact <LINE>
t5 snmp-server enable [server|traps]
t5 snmp-server host <IP>
t5 snmp-server location <LINE>

```

### Parameters

```
t5 snmp-server [community|contact|enable|host|location]
```

|                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| community <COMMUNITY-NAME> [ro rw] | <p>Defines a public or private community designation. By default, SNMPv2 community strings on most devices are set to public, for the read-only community string, and private for the read-write community string.</p> <ul style="list-style-type: none"> <li>• &lt;COMMUNITY-NAME&gt; – Specify the SNMP community name, and configure the access permission for this community string (used by devices to retrieve or modify information). <ul style="list-style-type: none"> <li>• ro – Allows a remote device to retrieve information only</li> <li>• rw – Allows a remote device to retrieve information and modify settings</li> </ul> </li> </ul> |
| <SNMP-STATION-IP>                  | Specify the SNMP management station IP address for receiving trap information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

t5 snmp-server contact <LINE>

|                |                                                                                                                                                                                                                       |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| contact <LINE> | <p>Configures the administrator of SNMP trap events for the T5 controller.</p> <ul style="list-style-type: none"> <li>• &lt;LINE&gt; – Specify the administrator’s name (should not exceed 64 characters).</li> </ul> |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

t5 snmp-server enable [server|traps]

|                       |                                                                                                                                                                                                                                                                                                                                 |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| enable [server traps] | <p>Enables the following:</p> <ul style="list-style-type: none"> <li>• server – Enables the SNMP server. When enabled, the system accepts SNMP management data. This option is enabled by default.</li> <li>• traps – Enables SNMP traps. When enabled, the system generates SNMP traps. This is enabled by default.</li> </ul> |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

t5 snmp-server host <IP>

|           |                                                                                                                                                                                                      |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| host <IP> | <p>Configures the T5 SNMP host’s IP address. The SNMP host receives the SNMP notifications.</p> <ul style="list-style-type: none"> <li>• &lt;IP&gt; – Specify the SNMP host’s IP address.</li> </ul> |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

t5 snmp-server location <LINE>

|                 |                                                                                                                                                                                           |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| location <LINE> | <p>Configures the system location for SNMP traps</p> <ul style="list-style-type: none"> <li>• &lt;LINE&gt; – Specify the SNMP trap location (should not exceed 64 characters).</li> </ul> |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Example

```

nx9500-6C8809(config-management-policy-test)#t5 snmp-server community lab rw 192.168.13.7
nx9500-6C8809(config-management-policy-test)#show context
management-policy test
 http server
 no ssh
 t5 snmp-server community lab rw 192.168.13.7
nx9500-6C8809(config-management-policy-test)#

```

### Related Commands

|    |                                                             |
|----|-------------------------------------------------------------|
| no | Removes or reverts SNMP server configuration for T5 devices |
|----|-------------------------------------------------------------|

## telnet

Enables Telnet. Telnet provides a command line interface to a remote host over TCP. Telnet provides no encryption, but it does provide a measure of authentication. Telnet access is disabled by default.

By default Telnet, when enabled, uses TCP (Transmission Control Protocol) port 23. Use this command to change the TCP port.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
telnet {port <1-65535>}
```

### Parameters

```
telnet {port <1-65535>}
```

|                |                                                                                                                                                                                                               |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| telnet         | Enables Telnet                                                                                                                                                                                                |
| port <1-65535> | Optional. Configures the Telnet port. This is the port used for Telnet connections. <ul style="list-style-type: none"><li>• &lt;1-65535&gt; – Sets a value from 1 - 165535. The default port is 23.</li></ul> |

### Examples

```
rfs4000-6DB5D4(config-management-policy-test)#telnet port 200
rfs4000-6DB5D4(config-management-policy-test)#show context
management-policy test
 telnet port 200
 no http server
 https server
 ftp username superuser password 1
 626b4033263d6d2ae4e79c48cdfcccb60fd4c77a8da9e365060597a6d6570ec2 rootdir dir
 ssh port 162
 snmp-server community snmpl ro
 snmp-server user snmpmanager v3 encrypted des auth md5 0 test123
 snmp-server host 172.16.10.23 v3 162
 aaa-login radius external
 aaa-login radius policy test
 idle-session-timeout 0
 restrict-access host 172.16.10.2 log all
rfs4000-6DB5D4(config-management-policy-test)#
```

### Related Commands

|    |                 |
|----|-----------------|
| no | Disables Telnet |
|----|-----------------|

## user (management-policy)

Adds new user account. Use this option to add a new user, and define the role, access type, and allowed locations assigned to the user.

Management services like Telnet, SSHv2, HTTP, HTTPS and FTP require users (administrators) enter a valid username and password, which is authenticated locally or centrally on a RADIUS server. SNMPv3 also requires a valid username and password, which is authenticated by the SNMPv3 module. For CLI users, the controller or service platform also requires user role information to know what permissions to assign.

- If local authentication is used, associated role information is defined on the controller or service platform when the user account is created.
- If RADIUS is used, role information is supplied by RADIUS using vendor-specific return attributes. If no role information is supplied by RADIUS, the controller or service platform applies default read-only permissions.

Administrators can limit users to specific management interfaces. During authentication, the controller or service platform looks at the user's access assignment to determine if the user has permissions to access an interface:

- If local authentication is used, role information is defined on the controller or service platform when the user account is created.
- If RADIUS is used, role information is supplied by RADIUS using vendor-specific return attributes.

The controller or service platform authenticates users using the integrated local database. When user credentials are presented the controller or service platform validates the username and password against the local database and assigns permissions based on the associated roles assigned. The controller or service platform can also deny the authentication request if the user is attempting to access a management interface not specified in the account's access mode list.

#### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### **Syntax**

```
user <USERNAME> password [0 <PASSWORD>|1 <SHA1-PASSWORD>|<PASSWORD>] role [device-
provisioning-admin|helpdesk|monitor|network-admin|security-admin|superuser|
system-admin|vendor-admin|web-user-admin]
user <USERNAME> password [0 <PASSWORD>|1 <SHA1-PASSWORD>|<PASSWORD>] role [device-
provisioning-admin|helpdesk|monitor|network-admin|security-admin|superuser|
system-admin|web-user-admin] access [all|console|ssh|telnet|web] ({allowed-locations
<ALLOWED-LOCATIONS>})
user <USERNAME> password [0 <PASSWORD>|1 <SHA1-PASSWORD>|<PASSWORD>] role vendor-admin
group <VENDOR-GROUP-NAME>
```

#### **Parameters**

```
user <USERNAME> password [0 <PASSWORD>|1 <SHA1-PASSWORD>|<PASSWORD>] role [device-
provisioning-admin|helpdesk|monitor|network-admin|security-admin|
superuser|system-admin|web-user-admin] access [all|console|ssh|telnet|web] ({allowed-
locations <ALLOWED-LOCATIONS>})
```

|                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| user <USERNAME>                                        | <p>Adds a new user account to this management policy</p> <ul style="list-style-type: none"> <li>• &lt;USERNAME&gt; – Sets the username. This is a mandatory field and cannot exceed 32 characters. Assign a name representative of the user and the intended role.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| password [0 <PASSWORD>] 1 <SHA1-PASSWORD>  <PASSWORD>] | <p>Configures a password</p> <ul style="list-style-type: none"> <li>• 0 &lt;PASSWORD&gt; – Sets a clear text password</li> <li>• 1 &lt;SHA1-PASSWORD&gt; – Sets the SHA1 hash of the password <ul style="list-style-type: none"> <li>• &lt;PASSWORD&gt; – Sets the password</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| role                                                   | <p>Configures the user role. The options are:</p> <ul style="list-style-type: none"> <li>• device-provisioning-admin – Device provisioning administrator. Has privileges to update (provision) device configuration files or firmware. Such updates run the risk of overwriting and losing a devices existing configuration unless the configuration is properly archived.</li> <li>• helpdesk – Helpdesk administrator. Performs troubleshooting tasks, such as run troubleshooting utilities (like a sniffer), view/retrieve logs, clear statistics, reboot, create and copy technical support dumps. The helpdesk administrator can also create a guest user account and password for registration. However, the helpdesk admin cannot execute controller or service platform reloads.</li> <li>• monitor – Monitor. Has read-only access to the system. Can view configuration and statistics except for secret information.</li> <li>• network-admin – Network administrator. Manages layer 2, layer 3, Wireless, RADIUS server, DHCP server, and Smart RF.</li> <li>• security-admin – Security administrator. Modifies WLAN keys and passphrases.</li> <li>• superuser – Superuser. Has full access, including halt and delete startup-config.</li> <li>• system-admin – System administrator. Upgrades image, boot partition, time, and manages admin access.</li> <li>• web-user-admin – Web user administrator. This role is used to create guest users and credentials. The Web user admin can access only the custom GUI screen and does not have access to the normal CLI and GUI.</li> </ul> |
| access [all console ssh  telnet  web]                  | <p>Configures the access type</p> <ul style="list-style-type: none"> <li>• all – Allows all types of access: console, SSH, Telnet, and Web</li> <li>• console – Allows console access only</li> <li>• ssh – Allows SSH access only</li> <li>• telnet – Allows Telnet access only</li> <li>• web – Allows Web access only</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| allowed-locations <ALLOWED-LOCATIONS>                  | <p>Optional. This keyword is recursive and optional. It configures a list of locations (either as a path or a RF Domain) to which this user is allowed access.</p> <ul style="list-style-type: none"> <li>• &lt;ALLOWED-LOCATIONS&gt; – Specify the allowed locations.</li> </ul> <p><b>Note:</b> Use this option to configure a list of RF Domains or its tree nodes to which this user is allowed access with respect to the Nsight policy.</p> <p><b>Note:</b> This option is not applicable to the user role 'web-user-admin'.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

```
user <USERNAME> password [0 <PASSWORD>|1 <SHA1-PASSWORD>|<PASSWORD>] role vendor-admin
group <VENDOR-GROUP-NAME>
```

|                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| user <USERNAME>                                        | <p>Adds a new user account to this management policy</p> <ul style="list-style-type: none"> <li>• &lt;USERNAME&gt; – Sets the username. This is a mandatory field and cannot exceed 32 characters. Assign a name representative of the user and the intended role.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| password [0 <PASSWORD>] 1 <SHA1-PASSWORD>  <PASSWORD>] | <p>Configures a password</p> <ul style="list-style-type: none"> <li>• 0 &lt;PASSWORD&gt; – Sets a clear text password 1 &lt;SHA1-PASSWORD&gt; – Sets the SHA1 hash of the password</li> <li>• &lt;PASSWORD&gt; – Sets the password</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| role vendor-admin                                      | <p>Configures this user's role as vendor-admin. Once created, the vendor-admin can access the online device-registration portal to add devices to the RADIUS vendor group to which he/she belongs. Vendor-admins have only Web access to the device registration portal.</p> <p>The WiNG software allows multiple vendors to securely on-board their devices through a single SSID. Each vendor has a 'vendor-admin' user who is assigned a unique, username/password credential for RADIUS server validation. Successfully validated vendor-admins can on-board their devices, which are, on completion of the on-boarding process, immediately placed on the vendor-allowed VLAN. On subsequent associations with this SSID, registered devices are dynamically placed into the vendor-allowed VLAN.</p> <p>If assigning the vendor-admin role, provide the vendor's group name for RADIUS authentication. The vendor's group takes precedence over the statically configured group for device registration.</p> <p><b>Note:</b> Use the <b>service &gt; show &gt; wireless &gt; credential-cache</b> command to view on-boarded device's VLAN assignment. Ensure that the REST server is enabled, to allow vendor users access to the online device registration portal.</p> <p><b>Note:</b> Note, by default the REST server is enabled. For more information, see <a href="#">rest-server</a>.</p> |
| group <VENDOR-GROUP-NAME>                              | <p>Associates this vendor-admin user with a vendor group, required for RADIUS authentication. The vendor group should be existing and configured in the RADIUS group policy. For more information on configuring RADIUS groups, see <a href="#">radius-group</a> on page 1551.</p> <ul style="list-style-type: none"> <li>• &lt;VENDOR-GROUP-NAME&gt; – Provide the vendor group name. In case of multiple allowed groups, provide a list of comma-separated group names.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Examples

```
rfs4000-6DB5D4(config-management-policy-test)#user TESTER password test123 role
superuser access all
rfs4000-6DB5D4(config-management-policy-test)#show context
management-policy test
telnet port 200
no http server
https server
ftp username superuser password 1
f617ca50c59fb47028f96db4baab5f3d8f03c03ab257960b0fd127c69f02cd7e rootdir dir
ssh port 162
user TESTER password 1 b6b37c51405f4e93c67fe8af82d450c9fd6af69324cd56a55055cfe695b6a14
role superuser access all
snmp-server community snmp1 ro
snmp-server user snmpmanager v3 encrypted des auth md5 0 test@123
snmp-server host 172.16.10.23 v3 162
aaa-login radius external
aaa-login radius policy test
idle-session-timeout 0
```

```

restrict-access host 172.16.10.2 log all
rfs4000-6DB5D4(config-management-policy-test)#
nx9500-6C8809(config-management-policy-OB)#user test password 0 test123 role vendor-admin
group Apple,Sony,Samsung
nx9500-6C8809(config-management-policy-OB)#user Samsung password 0 samsung role vendor-
admin group Samsung
nx9500-6C8809(config-management-policy-OB)#show context
management-policy OB
no telnet
no http server
https server
rest-server
ssh
user admin password 1 d9849649218dcaa79109fbd47bbf1a24ecdffleda220d21f76ce4c15a4e7e696
role superuser access all
user test password 1 62fca173a1ffc0e9cc4eef782b1978a5e0c47f66bc57a32992f03e3e00fe0bc4
role vendor-admin group Apple,Sony,Samsung
user Samsung password 1 39cb036b8e09c2ec625ebcda6e4001f4584263ed86fa69fc1f6b284113772eb0
role vendor-admin group Samsung
nx9500-6C8809(config-management-policy-OB)#

```

## Related Commands

|                 |                        |
|-----------------|------------------------|
| <code>no</code> | Removes a user account |
|-----------------|------------------------|

## service

Invokes service commands

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```

service [prompt|show]
service [prompt crash-info|show cli]

```

### Parameters

```

service [prompt crash-info|show cli]

```

|                           |                                                                                                                                                                                             |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| service prompt crash-info | Updates CLI prompt settings <ul style="list-style-type: none"> <li>• crash-info – Includes an asterisk at the end of the prompt if the device has crashfiles in flash:/crashinfo</li> </ul> |
| service show cli          | Displays running system information <ul style="list-style-type: none"> <li>• cli – Displays the current mode's CLI tree</li> </ul>                                                          |

### Examples

```

nx9500-6C8809(config-management-policy-default)#service show cli
Management Mode mode:
+-help [help]
+-search
+-WORD [help search WORD (|detailed|only-show|skip-show|skip-no)]

```



```

++detailed [help search WORD (|detailed|only-show|skip-show|skip-no)]
++only-show [help search WORD (|detailed|only-show|skip-show|skip-no)]
++skip-show [help search WORD (|detailed|only-show|skip-show|skip-no)]
++skip-no [help search WORD (|detailed|only-show|skip-show|skip-no)]
+-show
+-commands [show commands]
+-adoption
+-log
+-adoptee [show adoption log adoptee(|on DEVICE-NAME)]
+-on
+-DEVICE-NAME [show adoption log adoptee(|on DEVICE-NAME)]
+-adopter [show adoption log adopter (|mac AA-BB-CC-DD-EE-FF)(|on DEVICE-NAME)]
+-mac
+-AA-BB-CC-DD-EE-FF [show adoption log adopter (|mac AA-BB-CC-DD-EE-FF)(|on
DEVICE-NAME)]
+-on
+-DEVICE-NAME [show adoption log adopter (|mac AA-BB-CC-DD-EE-FF)(|on DEVICE-
NAME)]
--More--
nx9500-6C8809(config-management-policy-default)#

```

## Related Commands

|                                                                                                |
|------------------------------------------------------------------------------------------------|
| <b>no</b> Disables the inclusion of an asterix indicator notifying the presence of crash files |
|------------------------------------------------------------------------------------------------|

### *no (management-policy)*

Negates a command or reverts values to their default. When used in the config management policy mode, the no command negates or reverts management policy settings.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```

no [aaa-login|allowed-locations|banner|ftp|http|https|idle-session-timeout|ipv6|
passwd-entry|privilege-mode-password|rest-server|restrict-access|snmp-server|ssh|t5|telnet|
user|service]
no aaa-login tacacs [accounting|authentication|authorization|fallback|policy]
no allowed-location <LOCATION-TAG>
no banner motd
no ftp {password/rootdir}
no http server
no https [server|sslv3|use-secure-ciphers-only]
no passwd-entry role [device-provisioning-admin|helpdesk|monitor|network-admin|
security-admin|superuser|system-admin|vendor-admin|web-user-admin]
no [idle-session-timeout|privilege-mode-password|rest-server|restrict-access]
no ipv6 restrict-access
no snmp-server [community|display-vlan-info-per-radio|enable|host|manager|
max-pending-requests|request-timeout|suppress-security-configuration-level|throttle|user]
no snmp-server [community <WORD>|display-vlan-info-per-radio|enable traps|host <IP>
{<1-65535>}|
manager [all|v1|v2|v3]|max-pending-requests|request-timeout|suppress-security-

```

```
configuration-level|
throttle|user [snmpmanager|snmpoperator|snmptrap]]
no ssh {login-grace-time/port/use-key}
no t5 snmp-server [community|enable|host]
no [telnet|user <USERNAME>]
no service prompt crash-info
```

## Parameters

```
no <PARAMETERS>
```

|                                                                                                   |
|---------------------------------------------------------------------------------------------------|
| no <PARAMETERS> Removes or reverts this Management policy settings based on the parameters passed |
|---------------------------------------------------------------------------------------------------|

## Examples

The following example shows the management policy 'test' settings before the 'no' commands are executed:

```
rfs4000-6DB5D4(config-management-policy-test)#show context
management-policy test
 http server
 https server
 ftp username superuser password 1
 7ccb4568cb83e54f1e402f785a78ee930a453afda152baaf7c2b79277f225872 rootdir dir
 no ssh
 aaa-login radius external
 aaa-login radius policy test
 idle-session-timeout 100
 banner motd "Have a Good Day"
rfs4000-6DB5D4(config-management-policy-test)#
rfs4000-6DB5D4(config-management-policy-test)#no banner motd
rfs4000-6DB5D4(config-management-policy-test)#no idle-session-timeout
rfs4000-6DB5D4(config-management-policy-test)#no http server
```

The following example shows the management policy 'test' settings after the 'no' commands are executed:

```
rfs4000-6DB5D4(config-management-policy-test)#show context
management-policy test
 no http server
 https server
 ftp username superuser password 1
 626b4033263d6d2ae4e79c48cdfcccb60fd4c77a8da9e365060597a6d6570ec2 rootdir dir
 no ssh
 aaa-login radius external
 aaa-login radius policy test
 idle-session-timeout 0
rfs4000-6DB5D4(config-management-policy-test)#
```

# RADIUS POLICY

## RADIUS-POLICY

---

This chapter summarizes the RADIUS group, server, and user policy commands in the CLI command structure.

RADIUS (Remote Authentication Dial-In User Service) is a client/server protocol and software that enables remote access servers to authenticate users and authorize their access to the network. RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS clients send authentication requests to the local RADIUS server containing user authentication and network service access information.

RADIUS enables centralized management of authentication data (usernames and passwords). When a client attempts to associate to a network, the authentication request is sent to the local RADIUS server. The authentication and encryption of communications takes place through the use of a shared secret password (not transmitted over the network).

The local RADIUS server stores the user database locally, and can optionally use a remote user database. It ensures higher accounting performance. It allows the configuration of multiple users, and assigns policies for group authorization.

Controllers and access points allow enforcement of user-based policies. User policies include dynamic VLAN assignment and access based on time of day. A certificate is required for EAP TTLS, PEAP and TLS RADIUS authentication (configured with the RADIUS service).

Dynamic VLAN assignment is achieved based on the RADIUS server response. A user who associates to WLAN1 (mapped to VLAN1) can be assigned a different VLAN after RADIUS server authentication. This dynamic VLAN assignment overrides the WLAN's VLAN ID to which the user associates.

The chapter is organized into the following sections:

- [radius-group](#) on page 1551
- [radius-server-policy](#) on page 1559
- [radius-user-pool-policy](#) on page 1576



### Note

The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (\_) character. In other words, the name of a device cannot contain an underscore.

---

## radius-group

This section describes RADIUS user group configuration commands.

The local RADIUS server allows the configuration of user groups with common user policies. User group names and associated users are stored in the local database. The user ID in the received access request

is mapped to the associated wireless group for authentication. The configuration of groups allows enforcement of the following policies that control user access:

- Assign a VLAN to the user upon successful authentication
- Define start and end of time (HH:MM) when the user is allowed to authenticate
- Define the SSID list to which a user, belonging to this group, is allowed to associate
- Define the days of the week the user is allowed to login
- Rate limit traffic (for non-management users)

RADIUS users are categorized into three groups: normal user, management user, and guest user. A RADIUS group not configured as management or guest is a normal user group. User access and role settings depends on the RADIUS group the user belongs.

Use the (config) instance to configure RADIUS group commands. This command creates a group within the existing RADIUS group. To navigate to the RADIUS group instance, use the following commands:

```
<DEVICE>(config)#radius-group <GROUP-NAME>
nx9500-6C8809(config)#radius-group test
nx9500-6C8809(config-radius-group-test)#?
Radius user group configuration commands:
 guest Make this group a Guest group
 no Negate a command or set its defaults
 policy Radius group access policy configuration
 rate-limit Set rate limit for group

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-radius-group-test)#
```



#### Note

The RADIUS group name cannot exceed 32 characters, and cannot be modified as part of the group edit process.

The following table summarizes RADIUS group configuration commands.

*Table: RADIUS-Group Config Mode Commands*

| Command                             | Description                                      |
|-------------------------------------|--------------------------------------------------|
| <a href="#">guest</a> on page 1553  | Enables guest access for the newly created group |
| <a href="#">policy</a> on page 1554 | Configures RADIUS group access policy parameters |

| Command                              | Description                                                                       |
|--------------------------------------|-----------------------------------------------------------------------------------|
| <code>rate-limit</code> on page 1557 | Sets the default rate limit per user in Kbps, and applies it to all enabled WLANs |
| <code>no</code> on page 1558         | Negates a command or reverts settings to their default                            |



#### Note

For more information on common commands (clear, commit, help, revert, service, show, write, and exit), see [COMMON COMMANDS](#) on page 640.



#### Note

The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (\_) character. In other words, the name of a device cannot contain an underscore.

### *guest*

Configures this group as a guest (non-management) group. A guest user group has temporary permissions to the controller's local RADIUS server. You can configure multiple guest user groups, each having a unique set of settings. Guest user groups cannot be made management groups with access and role permissions.

Guest users and policies are used for captive portal authorization to the network.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
guest
```

#### Parameters

None

#### Examples

```
nx9500-6C8809(config-radius-group-test)#guest
nx9500-6C8809(config-radius-group-test)#show context
radius-group test
 guest
nx9500-6C8809(config-radius-group-test)#
```

#### Related Commands

|                              |                                    |
|------------------------------|------------------------------------|
| <code>no</code> on page 1558 | Makes this group a non-guest group |
|------------------------------|------------------------------------|

## policy

Sets a RADIUS group's authorization settings, such as access day/time, WLANs, etc.



### Note

A user-based VLAN is effective only if dynamic VLAN authorization is enabled for the WLAN.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
policy [access|day|inactivity-timeout|role|session-time|ssid|time|vlan]
policy vlan <1-4094>
policy access [all|console|ssh|telnet|web]
policy access [all|console|ssh|telnet|web] {(all/console/ssh/telnet/web)}
policy day [all|fr|mo|sa|su|th|tu|we|weekdays] {(fr/mo/sa/su/th/tu/we/weekdays)}
policy inactivity-timeout <60-86400>
policy role [device-provisioning-admin|helpdesk|monitor|network-admin|security-admin|
superuser|system-admin|web-user-admin]
policy session-time <5-144000>
policy ssid <SSID>
policy time start <HH:MM> end <HH:MM>
```



### Note

Access and role settings are applicable only to a management group. They cannot be configured for a RADIUS non-management group.

### Parameters

```
policy vlan <1-4094>
```

vlan <1-4094>

Sets the guest RADIUS group's VLAN ID from 1 - 4094. The VLAN ID is representative of the shared SSID each group member (user) employs to inter-operate within the network (once authenticated by the local RADIUS server). This option applicable to a guest user group, which has guest access and temporary permissions to the local RADIUS server. The terms of the guest access can be set uniquely for each group. Guest user groups cannot be made management groups with unique access and role permissions.

**Note:** Enable dynamic VLAN assignment for the WLAN for the VLAN assignment to take effect.

```
policy access [all|console|ssh|telnet|web] {(all/console/ssh/telnet/web)}
```

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| access | <p>Configures access type for a management group. Management groups can be assigned unique access and role permissions.</p> <ul style="list-style-type: none"> <li>• all – Allows all access. Allows access to the console, ssh, telnet, and/or Web</li> <li>• console – Allows console access only</li> <li>• ssh – Allows SSH access only</li> <li>• telnet – Allows Telnet access only</li> <li>• web – Allows Web access only</li> </ul> <p>These parameters are recursive, and you can provide access to more than one component.</p> |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
policy role [device-provisioning-admin|helpdesk|monitor|network-admin|security-admin|
superuser|system-admin|web-user-admin]
```

|                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| role [device-provisioning-admin  helpdesk monitor network-admin  security-admin superuser system- admin web-user-admin] | <p>Configures the role assigned to a management RADIUS group. If a group is listed as a management group, it may also have a unique role assigned. Available roles include:</p> <ul style="list-style-type: none"> <li>• device-provisioning-admin – Device provisioning administrator. Has privileges to update (provision) device configuration files or firmware. Such updates run the risk of overwriting and losing a devices existing configuration unless the configuration is properly archived.</li> <li>• helpdesk – Helpdesk administrator. Performs troubleshooting tasks, such as clear statistics, reboot, create and copy tech support dumps. The helpdesk administrator can also create a guest user account and password for registration. These details can be e-mailed or sent as SMS to a mobile phone.</li> <li>• monitor – Monitor. Has read-only access to the network. Can view configuration and statistics except for secret information</li> <li>• network-admin – Network administrator. has wired and wireless access to the network. Manages layer 2, layer 3, Wireless, RADIUS server, DHCP server, and Smart RF</li> <li>• security-admin – Security administrator. Has full read/write access to the network. Modifies WLAN keys and passphrases</li> <li>• superuser – Superuser. Has full access, including halt and delete startup config</li> <li>• system-admin – System administrator. Upgrades image, boot partition, time, and manages admin access</li> <li>• web-user-admin – Web user administrator. This role is used to create guest users and credentials. The web-user-admin can access only the custom GUI screen and does not have access to the normal CLI and GUI.</li> </ul> |
|-------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
policy inactivity-timeout <60-86400>
```

|                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| policy inactivity-timeout <60-86400> | <p>Configures the inactivity time for this RADIUS group users. If a frame is not received from a client for the specified period, then the client's session is removed. When defined, this value is used instead of the captive-portal inactivity timeout. If the inactivity timeout is not configured in the radius-group context or the captive-portal context, the default timeout (60 seconds) is applied.</p> <ul style="list-style-type: none"> <li>• &lt;60-86400&gt; – Specify a value from 60 - 86400 seconds. This option is disabled by default.</li> </ul> |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
policy session-time <5-144000>
```

|                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>policy session-time &lt;5-144000&gt;</code> | <p>Configures the session duration for client's belonging to a specific vendor group. Once configured, this is the duration for which over-the-air, on-boarded, successfully authenticated devices, belonging to a vendor group, get online access. The session is removed on completion of this duration. The vendor's RADIUS group takes precedence over statically configured group for device registration.</p> <ul style="list-style-type: none"> <li>• &lt;5-144000&gt; – Specify a value from 5 - 144000 minutes. This option is disabled by default.</li> </ul> <p><b>Note:</b> For more information, see <a href="#">configuring-device-registration-with-dynamic-vlan-assignment</a> on page 329.</p> |
|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

`policy ssid <SSID>`

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>ssid &lt;SSID&gt;</code> | <p>Sets the SSID (Service Set Identifier) for this guest RADIUS group. Use this command to assign SSIDs that users within this RADIUS group are allowed to associate. Assign SSIDs of those WLANs only that the guest users need to access. This option is not available for a management group.</p> <ul style="list-style-type: none"> <li>• &lt;SSID&gt; – Specify a case-sensitive alphanumeric SSID, not exceeding 32 characters.</li> </ul> |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

`policy day [all|fr|mo|sa|su|th|tu|we|weekdays] {(fr|mo|sa|su|th|tu|we|weekdays)}`

|                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>day [all fr mo sa su th tu we weekdays] {(fr mo sa su th tu we weekdays)}</code> | <p>Configures the days on which this guest RADIUS group members can access the local RADIUS resources. The options are recursive, and you can provide access on multiple days.</p> <ul style="list-style-type: none"> <li>• fr – Allows access on Friday only</li> <li>• mo – Allows access on Mondays only</li> <li>• sa – Allows access on Saturdays only</li> <li>• su – Allows access on Sundays only</li> <li>• th – Allows access on Thursdays only</li> <li>• tu – Allows access on Tuesdays only</li> <li>• we – Allows access on Wednesdays only</li> <li>• weekdays – Allows access on weekdays only (Monday to Friday)</li> </ul> |
|----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

`policy time start <HH:MM> end <HH:MM>`

|                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>time start&lt;HH:MM&gt; end &lt;HH:MM&gt;</code> | <p>Configures the time when this RADIUS group can access the network</p> <ul style="list-style-type: none"> <li>• start &lt;HH:MM&gt; – Sets the start time in the HH:MM format (for example, 13:30 means the user can login only after 1:30 PM). Specifies the time users, within each listed group, can access the local RADIUS resources.</li> <li>• end &lt;HH:MM&gt; – Sets the end time in the HH:MM format (for example, 17:30 means the user is allowed to remain logged in until 5:30 PM). Specifies the time users, within each listed group, lose access to the local RADIUS resources.</li> </ul> |
|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Usage Guidelines**

A management group access policy provides:

- access details
- user role
- policy's start and end time





The SSID, day, and VLAN settings are not applicable to a management user group.

## Examples

The following example shows a RADIUS guest group settings:

```
nx9500-6C8809(config-radius-group-test)#policy time start 13:30 end 17:30
nx9500-6C8809(config-radius-group-test)#policy day all
nx9500-6C8809(config-radius-group-test)#policy vlan 1
nx9500-6C8809(config-radius-group-test)#policy ssid test
nx9500-6C8809(config-radius-group-test)#show context
radius-group test
 guest
 policy vlan 1
 policy ssid test
 policy day mo
 policy day tu
 policy day we
 policy day th
 policy day fr
 policy day sa
 policy day su
 policy time start 13:30 end 17:30
nx9500-6C8809(config-radius-group-test)#
```

The following example shows a RADIUS management group settings:

```
nx9500-6C8809(config-radius-group-management)#policy access console ssh telnet
nx9500-6C8809(config-radius-group-management)#policy role network-admin
nx9500-6C8809(config-radius-group-management)#policy time start 9:30 end 20:30
nx9500-6C8809(config-radius-group-management)#show context
radius-group management
 policy time start 9:30 end 20:30
 policy access console ssh telnet web
 policy role network-admin
nx9500-6C8809(config-radius-group-management)#
```

## Related Commands

|                              |                                                      |
|------------------------------|------------------------------------------------------|
| <code>no</code> on page 1558 | Removes or modifies a RADIUS group's access settings |
|------------------------------|------------------------------------------------------|

### *rate-limit*

Sets the rate limit for the guest RADIUS server group

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
rate-limit [from-air|to-air] <100-1000000>
```



#### Note

The rate-limit setting is not applicable to a management group.

## Parameters

rate-limit [from-air|to-air] <100-1000000>

|                        |                                                                                                                                                                                                        |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| to-air <100-1000000>   | Sets the rate limit in the downlink direction, from the network to the wireless client <ul style="list-style-type: none"><li>&lt;100-1000000&gt; - Specify the rate from 100 - 1000000 kbps.</li></ul> |
| from-air <100-1000000> | Sets the rate limit in the uplink direction, from the wireless client to the network <ul style="list-style-type: none"><li>&lt;100-1000000&gt; - Specify the rate from 100 - 1000000 kbps.</li></ul>   |

## Examples

```
nx9500-6C8809(config-radius-group-test)#rate-limit to-air 200
nx9500-6C8809(config-radius-group-test)#show context
radius-group test
 guest
 policy vlan 1
 policy ssid test
 policy day mo
 policy day tu
 policy day we
 policy day th
 policy day fr
 policy day sa
 policy day su
 rate-limit to-air 200
 policy time start 13:30 end 17:30
nx9500-6C8809(config-radius-group-test)#
```

## Related Commands

|                 |                                              |
|-----------------|----------------------------------------------|
| no on page 1558 | Removes the RADIUS guest group's rate limits |
|-----------------|----------------------------------------------|

*no*

Negates a command or sets its default. Removes or modifies the RADIUS group policy settings. When used in the config RADIUS group mode, the *no* command removes or modifies the following settings: access type, access days, role type, VLAN ID, and SSID.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
no [guest|policy|rate-limit]
no guest
no policy [access|day|inactivity-timeout|role|session-time|ssid|time|vlan]
no policy access [all|console|ssh|telnet|web]
no policy day [all|fr|mo|sa|su|th|tu|we|weekdays]
no policy session-time
no policy ssid [<SSID>|all]
no policy [inactivity-timeout|role|time|vlan]
no rate-limit [from-air|to-air]
```

## Parameters

no <PARAMETERS>

no <PARAMETERS> Negates a command or sets its default. Removes or modifies the RADIUS group policy settings. When used in the config RADIUS group mode, the no command removes or modifies the following settings: access type, access days, role type, VLAN ID, and SSID.

## Examples

The following example shows the RADIUS guest group 'test' settings before the 'no' commands are executed:

```
nx9500-6C8809(config-radius-group-test)#show context
radius-group test
 guest
 policy vlan 1
 policy ssid test
 policy day mo
 policy day tu
 policy day we
 policy day th
 policy day fr
 policy day sa
 policy day su
 rate-limit to-air 200
 policy time start 13:30 end 17:30
nx9500-6C8809(config-radius-group-test)#
nx9500-6C8809(config-radius-group-test)#no guest
nx9500-6C8809(config-radius-group-test)#no rate-limit to-air
nx9500-6C8809(config-radius-group-test)#no policy day all
```

The following example shows the RADIUS guest group 'test' settings after the 'no' commands are executed:

```
nx9500-6C8809(config-radius-group-test)#show context
radius-group test
 policy vlan 1
 policy ssid test
 policy time start 13:30 end 17:30
nx9500-6C8809(config-radius-group-test)#
```

## radius-server-policy

Creates an onboard device RADIUS server policy.

A RADIUS server policy is a unique authentication and authorization configuration that receives user connection requests, authenticates users, and returns configuration information necessary for the RADIUS client to deliver service to the user. The client is the entity with authentication information requiring validation. The local RADIUS server has access to a database of authentication information used to validate the client's authentication request.

The local RADIUS server uses authentication schemes like PAP, CHAP, or EAP to verify and confirm information provided by a user. The user's proof of identification is verified, along with, optionally, other information. A local RADIUS server policy can also be configured to refer to an external LDAP (Lightweight Directory Access Protocol) (LDAP) resource to verify a user's credentials.

Use the (config) instance to configure RADIUS-Server-Policy related parameters. To navigate to the RADIUS-Server-Policy instance, use the following commands:

```
<DEVICE>(config)#radius-server-policy <POLICY-NAME>
nx9500-6C8809(config)#radius-server-policy test
nx9500-6C8809(config-radius-server-policy-test)#?
Radius Configuration commands:
 authentication Radius authentication
 bypass Bypass Certificate Revocation List(CRL) check
 chase-referral Enable chasing referrals from LDAP server
 crl-check Enable Certificate Revocation List(CRL) check
 ldap-agent LDAP Agent configuration parameters
 ldap-group-verification Enable LDAP Group Verification setting
 ldap-server LDAP server parameters
 local RADIUS local realm
 nas RADIUS client
 no Negate a command or set its defaults
 proxy RADIUS proxy server
 session-resumption Enable session resumption/fast reauthentication by
 using cached attributes
 termination Enable Eap termination for proxy requests
 use Set setting to use

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-radius-server-policy-test)#
```

The following table summarizes RADIUS server policy configuration commands.

*Table: RADIUS-Server-Policy Config Mode Commands*

| Commands                                             | Description                                                                                                                           |
|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">authentication</a> on page 1561          | Configures RADIUS authentication settings                                                                                             |
| <a href="#">bypass</a> on page 1562                  | Enables bypassing of CRL check                                                                                                        |
| <a href="#">chase-referral</a> on page 1563          | Enables LDAP server referral chasing                                                                                                  |
| <a href="#">crl-check</a> on page 1564               | Enables a CRL (certificate revocation list ) check                                                                                    |
| <a href="#">ldap-agent</a> on page 1565              | Configures the LDAP agent settings                                                                                                    |
| <a href="#">ldap-group-verification</a> on page 1566 | Enables LDAP group verification                                                                                                       |
| <a href="#">ldap-server</a> on page 1567             | Configures the LDAP server settings                                                                                                   |
| <a href="#">local</a> on page 1569                   | Configures a local RADIUS realm                                                                                                       |
| <a href="#">nas</a> on page 1570                     | Configures the key sent to a RADIUS client                                                                                            |
| <a href="#">proxy</a> on page 1571                   | Configures the RADIUS proxy server's settings                                                                                         |
| <a href="#">session-resumption</a> on page 1572      | Enables session resumption                                                                                                            |
| <a href="#">termination</a> on page 1573             | Enables EAP termination on this current RADIUS server policy. When enabled, EAP authentication is terminated at the controller level. |

| Commands                      | Description                                           |
|-------------------------------|-------------------------------------------------------|
| <code>use</code> on page 1574 | Defines settings used with the RADIUS server policy   |
| <code>no</code> on page 1575  | Removes or resets the RADIUS server policy's settings |

## authentication

Specifies the RADIUS data source used for user authentication. Options include local for the local user database or LDAP for a remote LDAP resource.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
authentication [data-source|eap-auth-type]
authentication data-source [ldap|local]
authentication data-source [ldap {fallback}|local] {(ssid <SSID> precedence <1-5000>)}
authentication eap-auth-type [all|peap-gtc|peap-mschapv2|tls|ttls-md5|ttls-mschapv2|ttls-pap]
```

### Parameters

```
authentication data-source [ldap {fallback}|local] {(ssid <SSID> precedence <1-5000>)}
```

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| data-source   | The RADIUS sever can either use the local database or an external LDAP server to authenticate a user. It is necessary to specify the data source. The options are: <b>LDAP</b> and <b>local</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| ldap fallback | <p>Uses a remote LDAP server as the data source</p> <ul style="list-style-type: none"> <li>• fallback - Optional. Enables fallback to local authentication. This feature ensures that if the designated external LDAP resource were to fail or become unavailable, the client is authenticated against the local RADIUS resource. This option is disabled by default.</li> </ul> <p>When using LDAP as the authentication external source, PEAP-MSCHAPv2 authentication type can be used only if the LDAP server returns the password as plain-text. PEAP-MSCHAPv2 authentication is not supported if the LDAP server returns encrypted passwords. This restriction does not apply for Microsoft's Active Directory server.</p> |

|                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| local                                 | Uses the local user database to authenticate a user. This is the default setting.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| ssid <SSID><br>precedence<br><1-5000> | <p>The following keywords are recursive and common to both 'ldap' and 'local' parameters:</p> <ul style="list-style-type: none"> <li>• ssid – Optional. Associates the data source, selected in the previous step, with a SSID.</li> <li>• &lt;SSID&gt; – Specify the SSID for this authentication data source. The SSID is case sensitive and should not exceed 32 characters in length. Do not use any of the following characters (&lt; &gt;   " &amp; \ ? ,).</li> </ul> <p>precedence &lt;SSID&gt; – Sets the precedence for this authentication rule. The precedence value allows systematic evaluation and application of rules. Rules with the lowest precedence receive the highest priority.</p> <p>&lt;1-5000&gt; – Specify a precedence from 1 -5000.</p> <p><b>Note:</b> Specifying the SSID allows the RADIUS server to use the SSID attribute in access requests to determine the data source to use. This option is applicable to onboard RADIUS servers only.</p> |

```
authentication eap-auth-type [all|peap-gtc|peap-mschapv2|tls|ttls-md5|ttls-mschapv2|ttls-pap]
```

|               |                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| eap-auth-type | Uses EAP (Extensible Authentication Protocol), with this RADIUS server policy, for user authentication<br>The EAP authentication types supported by the local RADIUS server are: <b>all, peap-gtc, peap-mschapv2, tls, ttls-md5, ttls-mschapv2, ttls-pap.</b>                                                                                                                                      |
| all           | Enables both TTLS and PEAP authentication. This is the default setting.                                                                                                                                                                                                                                                                                                                            |
| peap-gtc      | Enables PEAP with default authentication using GTC                                                                                                                                                                                                                                                                                                                                                 |
| peap-mschapv2 | Enables PEAP with default authentication using MSCHAPv2<br>When using LDAP as the authentication external source, PEAP-MSCHAPv2 authentication type can be used only if the LDAP server returns the password as plain-text. PEAP-MSCHAPv2 authentication is not supported if the LDAP server returns encrypted passwords. This restriction does not apply for Microsoft's Active Directory server. |
| tls           | Enables TLS as the EAP type                                                                                                                                                                                                                                                                                                                                                                        |
| ttls-md5      | Enables TTLS with default authentication using md5                                                                                                                                                                                                                                                                                                                                                 |
| ttls-mschapv2 | Enables TTLS with default authentication using MSCHAPv2                                                                                                                                                                                                                                                                                                                                            |
| ttls-pap      | Enables TTLS with default authentication using PAP                                                                                                                                                                                                                                                                                                                                                 |

### Examples

```
nx9500-6C8809(config-radius-server-policy-test)#authentication eap-auth-type tls
nx9500-6C8809(config-radius-server-policy-test)#show context
radius-server-policy test
 authentication eap-auth-type tls
nx9500-6C8809(config-radius-server-policy-test)#
```

### Related Commands

|                 |                                            |
|-----------------|--------------------------------------------|
| no on page 1575 | Removes the RADIUS authentication settings |
|-----------------|--------------------------------------------|

### bypass

Enables bypassing of a CRL check. When enabled, this feature bypasses checks for missing and expired CRLs. This option is enabled by default.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
bypass [crl-check|expired-crl]
```

### Parameters

```
bypass [crl-check|expired-crl]
```

|                                |                                                                                                                                                                                                                                                                                                                  |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| bypass [crl-check expired-crl] | Bypasses CRL check based on the parameters passed <ul style="list-style-type: none"><li>• crl-check – Bypasses CRL check of missing CRLs</li><li>• expired-crl – Bypasses CRL check of expired CRLs</li></ul> <p><b>Note:</b> A CRL is a list of certificates that have been revoked or are no longer valid.</p> |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config-radius-server-policy-test)#bypass crl-check
nx9500-6C8809(config-radius-server-policy-test)##bypass expired-crl
nx9500-6C8809(config-radius-server-policy-test)#show context include-factory | include
bypass
 bypass expired-crl
 bypass crl-check
nx9500-6C8809(config-radius-server-policy-test)#
```

### Related Commands

|                 |                                                                 |
|-----------------|-----------------------------------------------------------------|
| no on page 1575 | Disables bypassing of checking for missing CRLs or expired CRLs |
|-----------------|-----------------------------------------------------------------|

### *chase-referral*

Enables chasing of referrals from an external LDAP server resource

An LDAP referral is a controller or service platform's way of indicating to a client it does not hold the section of the directory tree where a requested content object resides. The referral is the controller or service platform's direction to the client a different location is more likely to hold the object, which the client uses as the basis for a DNS search for a domain controller. Ideally, referrals always reference a domain controller that indeed holds the object. However, it is possible for the domain controller to generate another referral, although it usually does not take long to discover the object does not exist and inform the client.

This feature is disabled by default.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000

- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

chase-referral

### Parameters

None

### Examples

```
nx9500-6C8809(config-radius-server-policy-test)#chase-referral
```

### Related Commands

|                              |                                       |
|------------------------------|---------------------------------------|
| <code>no</code> on page 1575 | Disables LDAP server referral chasing |
|------------------------------|---------------------------------------|

### *crl-check*

Enables a CRL check on this RADIUS server policy. A CRL is a list of revoked certificates issued and subsequently revoked by a CA (Certification Authority). Certificates can be revoked for a number of reasons including failure or compromise of a device using a certificate, a compromise of a certificate key pair or errors within an issued certificate. The mechanism used for certificate revocation depends on the CA.

This option is disabled by default.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

crl-check

### Parameters

None

### Examples

```
nx9500-6C8809(config-radius-server-policy-test)#crl-check
nx9500-6C8809(config-radius-server-policy-test)#show context
radius-server-policy test
 authentication eap-auth-type tls
 crl-check
nx9500-6C8809(config-radius-server-policy-test)#
```

### Related Commands

|                              |                                              |
|------------------------------|----------------------------------------------|
| <code>no</code> on page 1575 | Disables CRL check on a RADIUS server policy |
|------------------------------|----------------------------------------------|



## ldap-agent

Configures the LDAP agent's settings in the RADIUS server policy context

When a user's credentials are stored on an external LDAP server, the local RADIUS server cannot successfully conduct PEAP-MSCHAPv2 authentication, since it is not aware of the user's credentials maintained on the external LDAP server resource. Therefore, up to two LDAP agents can be provided locally so remote LDAP authentication can be successfully accomplished on the remote LDAP resource (using credentials maintained locally).

This feature is available to all controller, service platforms and access point models.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
ldap-agent [join|join-retry-timeout|primary|secondary]
ldap-agent [join {on <DEVICE-NAME>}|join-retry-timeout <60-300>]
ldap-agent [primary|secondary] domain-name <LDAP-DOMAIN-NAME> domain-admin-user
<ADMIN-USER-NAME> domain-admin-password [0 <WORD>|2 <WORD>]
```

### Parameters

```
ldap-agent [join {on <DEVICE-NAME>}|join-retry-timeout <60-300>]
```

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ldap-agent                  | Configures the LDAP agent's settings                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| join {on <DEVICE-NAME>}     | Initiates the join process, which binds the RADIUS server with the LDAP server's (Windows) domain. When successful, the hostname (name of the AP, wireless controller, or service platform) is added to the LDAP server's Active Directory. <ul style="list-style-type: none"><li>• on &lt;DEVICE-NAME&gt; - Optional. Specifies the device name<ul style="list-style-type: none"><li>• &lt;DEVICE-NAME&gt; - Specify the name of the AP, wireless controller, or service platform.</li></ul></li></ul> <p><b>Note:</b> To confirm the join status of a controller, use the <b>show &gt; ldap-agent &gt; join-status</b> command.</p> |
| join-retry-timeout <60-300> | If the join process fails (i.e. the RADIUS server fails to join the LDAP server's domain), the process is retried after a specified interval. This command configures the interval (in seconds) between two successive join attempts. <ul style="list-style-type: none"><li>• &lt;60-300&gt; - Set the timeout value from 60 - 300 seconds. The default is 60 seconds.</li></ul> <p><b>Note:</b> A retry timer is initiated as soon as the join process starts, which tracks the time lapse in case of a failure.</p>                                                                                                                 |

```
ldap-agent [primary|secondary] domain-name <LDAP-DOMAIN-NAME> domain-admin-user
<ADMIN-USER-NAME> domain-admin-password [0 <WORD>|2 <WORD>]
```

|            |                                                                                                                                                                          |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ldap-agent | Configures the LDAP agent's settings                                                                                                                                     |
| primary    | Configures the primary LDAP server details, such as domain name, user name, and password. The RADIUS server uses these credentials to bind with the primary LDAP server. |

|                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| secondary                                        | Configures the secondary LDAP server details, such as domain name, user name, and password. The RADIUS server uses these credentials to bind with the secondary LDAP server.                                                                                                                                                                                                                                           |
| domain-name<br><LDAP-DOMAIN-NAME>                | This keyword is common to both the 'primary' and 'secondary' parameters. <ul style="list-style-type: none"> <li>domain-name - Configures the primary or secondary LDAP server's domain name <ul style="list-style-type: none"> <li>&lt;LDAP-DOMAIN-NAME&gt; - Specify the domain name.</li> </ul> </li> </ul>                                                                                                          |
| domain-admin-user<br><ADMIN-USER-NAME>           | This keyword is common to both the 'primary' and 'secondary' parameters. <ul style="list-style-type: none"> <li>domain-admin-user - Configures the primary or secondary LDAP server's admin user name <ul style="list-style-type: none"> <li>&lt;ADMIN-USER-NAME&gt; - Specify the admin user's name.</li> </ul> </li> </ul>                                                                                           |
| domain-admin-password [0<br><WORD>  2<br><WORD>] | This keyword is common to both the 'primary' and 'secondary' parameters. <ul style="list-style-type: none"> <li>domain-admin-password - Configures the primary or secondary LDAP server's admin user password <ul style="list-style-type: none"> <li>0 &lt;WORD&gt; - Specifies the password in the unencrypted format</li> <li>2 &lt;WORD&gt; - Specifies the password in the encrypted format</li> </ul> </li> </ul> |

### Examples

```
rfs4000-229D58(config-radius-server-policy-test)#ldap-agent primary domain-name
test domain-admin-user Administrator domain-admin-password 0 test@123
rfs4000-229D58(config-radius-server-policy-test)#show context
radius-server-policy test
 ldap-agent primary domain-name test domain-admin-user Administrator domain-admin-password
0 test@123
rfs4000-229D58(config-radius-server-policy-test)#
```

### Related Commands

|                              |                                                            |
|------------------------------|------------------------------------------------------------|
| <code>no</code> on page 1575 | Removes LDAP agent settings from this RADIUS server policy |
|------------------------------|------------------------------------------------------------|

### *ldap-group-verification*

Enables LDAP group verification settings on this RADIUS server policy. This option is enabled by default.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
ldap-group-verification
```

### Parameters

None

### Examples

```
nx9500-6C8809(config-radius-server-policy-test)#ldap-group-verification
nx9500-6C8809(config-radius-server-policy-test)#show context include-factory | include
ldap-group-verification
```

```
ldap-group-verification
nx9500-6C8809(config-radius-server-policy-test)#
```

## Related Commands

|                 |                                           |
|-----------------|-------------------------------------------|
| no on page 1575 | Disables LDAP group verification settings |
|-----------------|-------------------------------------------|

### ldap-server

Configures the LDAP server's settings. Configuring LDAP server allows users to login and authenticate from anywhere on the network.

Administrators have the option of using the local RADIUS server to authenticate users against an external LDAP server resource. Using an external LDAP user database allows the centralization of user information and reduces administrative user management overhead making RADIUS authorization more secure and efficient.

RADIUS is not just a database. It is a protocol for asking intelligent questions to a user database (like LDAP). LDAP however is just a database of user credentials used optionally with the local RADIUS server to free up resources and manage user credentials from a secure remote location. It is the local RADIUS resources that provide the tools to perform user authentication and authorize users based on complex checks and logic. A LDAP user database alone cannot perform such complex authorization checks.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
ldap-server [dead-period|primary|secondary]
ldap-server dead-period <0-600>
ldap-server [primary|secondary] host <IP> port <1-65535> login <LOGIN-NAME>
bind-dn <BIND-DN> base-dn <BASE-DN> passwd [0 <PASSWORD>|2 <ENCRYPTED-PASSWORD>|
<PASSWORD>]
passwd-attr <ATTR> group-attr <ATTR> group-filter <FILTER> group-membership <WORD>
{net-timeout <1-10>/start-tls net-timeout <1-10>/tls-mode net-timeout <1-10>}
```

### Parameters

```
ldap-server dead-period <0-600>
```

|                        |                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dead-period<br><0-600> | Sets an interval, in seconds, during which the local server does not contact its LDAP server resource once its been defined as unavailable. A dead period is only implemented when additional LDAP servers are configured and available. <ul style="list-style-type: none"><li>• &lt;0-600&gt; - Specify a value from 0 - 600 seconds. The default is 300 seconds.</li></ul> |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
ldap-server [primary|secondary] host <IP> port <1-65535> login <LOGIN-NAME>
bind-dn <BIND-DN> base-dn <BASE-DN> passwd [0 <PASSWORD>|2 <ENCRYPTED-PASSWORD>|
<PASSWORD>]
passwd-attr <ATTR> group-attr <ATTR> group-filter <FILTER> group-membership <WORD>
{net-timeout <1-10>/start-tls net-timeout <1-10>/tls-mode net-timeout <1-10>}
```

|                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ldap primary                                                           | Configures the primary LDAP server settings                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| ldap secondary                                                         | Configures the secondary LDAP server settings                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| host <IP>                                                              | Specifies the LDAP host's IP address <ul style="list-style-type: none"> <li>• &lt;IP&gt; – Specify the LDAP server's IP address.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| port <1-65535>                                                         | Configures the LDAP server port <ul style="list-style-type: none"> <li>• &lt;1-65535&gt; – Specify a port between 1 - 65535.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| login <LOGIN-NAME>                                                     | Configures the login name of a user to access the LDAP server <ul style="list-style-type: none"> <li>• &lt;LOGIN-NAME&gt; – Specify a login ID (should not exceed 127 characters).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| bind-dn <BIND-DN>                                                      | Configures a distinguished bind name. This is the DN (distinguished name) used to bind with the LDAP server. The DN is the name that uniquely identifies an entry in the LDAP directory. A DN is made up of attribute value pairs, separated by commas. <ul style="list-style-type: none"> <li>• &lt;BIND-DN&gt; – Specify a bind name (should not exceed 127 characters)</li> </ul>                                                                                                                                                                                                                                                                      |
| base-dn <BASE-DN>                                                      | Configures a distinguished base name. This is the DN that establishes the base object for the search. The base object is the point in the LDAP tree at which to start searching. LDAP DNs begin with a specific attribute (usually some sort of name), and continue with progressively broader attributes, often ending with a country attribute. The first component of the DN is referred to as the RDN (Relative Distinguished Name). It identifies an entry distinctly from any other entries that have the same parent <ul style="list-style-type: none"> <li>• &lt;BASE-DN&gt; – Specify a base name (should not exceed 127 characters).</li> </ul> |
| passwd [0<br><PASSWORD>  2<br><ENCRYPTED-<br>PASSWORD> <br><PASSWORD>] | Sets a valid password for the LDAP server. <ul style="list-style-type: none"> <li>• 0 &lt;PASSWORD&gt; – Sets an UNENCRYPTED password</li> <li>• 2 &lt;PASSWORD&gt; – Sets an ENCRYPTED password</li> <li>• &lt;PASSWORD&gt; – Sets the LDAP server bind password, specified UNENCRYPTED, with a maximum size of 31 characters</li> </ul>                                                                                                                                                                                                                                                                                                                 |
| passwd-attr <ATTR>                                                     | Specify the LDAP server password attribute (should not exceed 63 characters).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| group-attr <ATTR>                                                      | Specify a name to configure group attributes (should not exceed 31 characters). LDAP systems have the facility to poll dynamic groups. In an LDAP dynamic group an administrator can specify search criteria. All users matching the search criteria are considered a member of this dynamic group. Specify a group attribute used by the LDAP server. An attribute could be a group name, group ID, password or group membership name.                                                                                                                                                                                                                   |
| group-filter <FILTER>                                                  | Specify a name for the group filter attribute (should not exceed 255 characters). This filter is typically used for security role-to-group assignments and specifies the property to look up groups in the directory service.                                                                                                                                                                                                                                                                                                                                                                                                                             |
| group-membership<br><WORD>                                             | Specify a name for the group membership attribute (should not exceed 63 characters). This attribute is sent to the LDAP server when authenticating users.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| net-time <1-10>                                                        | Optional. Select a value from 1 - 10 to configure the network timeout (number of seconds to wait for a response from the target primary or secondary LDAP server). The default is 10 seconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| start-tls net-timeout<br><1-10>                                        | Optional. Select a value from 1 - 10 to configure the network timeout for secure communication using start_tls support on the external LDAP server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| tls-mode net-timeout<br><1-10>                                         | Optional. Select a value from 1 - 10 to configure the network timeout for secure communication using tls_mode support on the external LDAP server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## Examples

```
nx9500-6C8809(config-radius-server-policy-test)#ldap-server dead-period 100
nx9500-6C8809(config-radius-server-policy-test)#ldap-server primary host 172.16.10.19 port
162 login test bind-dn bind-dn1 base-dn base-dn1 passwd 0 test@123 passwd-attr test123
group-attr group1 group-filter groupfilter1
group-membership groupmembershipl net-timeout 2
nx9500-6C8809(config-radius-server-policy-test)#show context
radius-server-policy test
 authentication eap-auth-type tls
 crl-check
 ldap-server primary host 172.16.10.19 port 162 login "test" bind-dn "bind-dn1" base-dn
"base-dn1" passwd 0 test@123 passwd-attr test123 group-attr group1 group-filter
"groupfilter1" group-membership groupmembershipl net-timeout 2
 ldap-server dead-period 100nx9500-6C8809(config-radius-server-policy-test)#
```

## Related Commands

|                              |                                     |
|------------------------------|-------------------------------------|
| <code>no</code> on page 1575 | Disables the LDAP server parameters |
|------------------------------|-------------------------------------|

## *local*

Configures a local RADIUS realm on this RADIUS server policy

When the local RADIUS server receives a request for a user name with a realm, the server references a table of realms. If the realm is known, the server proxies the request to the RADIUS server.

## Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
local realm <RADIUS-REALM>
```

## Parameters

```
local realm <RADIUS-REALM>
```

|                      |                                                                                                                                                                                |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| realm <RADIUS-REALM> | Configures a local RADIUS realm <ul style="list-style-type: none"><li>• &lt;RADIUS-REALM&gt; - Sets a local RADIUS realm name (a string not exceeding 50 characters)</li></ul> |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-radius-server-policy-test)#local realm realm1
nx9500-6C8809(config-radius-server-policy-test)#show context
radius-server-policy test
 authentication eap-auth-type tls
 crl-check
 local realm realm1
 ldap-server primary host 172.16.10.19 port 162 login "test" bind-dn "bind-dn1" base-dn
"base-dn1" passwd 0 test@123 passwd-attr test123 group-attr group1 group-filter
"groupfilter1" group-membership groupmembershipl net-timeout 2
 ldap-server dead-period 100
nx9500-6C8809(config-radius-server-policy-test)#
```

## Related Commands

`no` on page 1575

Removes the RADIUS local realm

*nas*

Configures the key sent to a RADIUS client.

A RADIUS client is a mechanism to communicate with a central server to authenticate users and authorize access to the controller, service platform or access point managed network.

The client and server share a secret (a password). That shared secret followed by the request authenticator is put through a MD5 hash algorithm to create a 16 octet value which is XORed with the password entered by the user. If the user password is greater than 16 octets, additional MD5 calculations are performed, using the previous ciphertext instead of the request authenticator. The server receives a RADIUS access request packet and verifies the server possesses a shared secret for the client. If the server does not possess a shared secret for the client, the request is dropped. If the client received a verified access accept packet, the username and password are considered correct, and the user is authenticated. If the client receives a verified access reject message, the username and password are considered to be incorrect, and the user is not authenticated.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
nas <IP/M> secret [0|2|<LINE>]
nas <IP/M> secret [0 <LINE>|2 <LINE>|<LINE>]
```

### Parameters

```
nas <IP/M> secret [0 <LINE>|2 <LINE>|<LINE>]
```

|                                   |                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IP/M>                            | Sets the RADIUS client's IP address <ul style="list-style-type: none"><li>• &lt;IP/M&gt; - Sets the RADIUS client's IP address in the A.B.C.D/M format</li></ul>                                                                                                                                                   |
| secret [0 <LINE> 2 <LINE> <LINE>] | Sets the RADIUS client's shared secret. Use one of the following options: <ul style="list-style-type: none"><li>• 0 &lt;LINE&gt; - Sets an UNENCRYPTED secret</li><li>• 2 &lt;LINE&gt; - Sets an ENCRYPTED secret</li><li>• &lt;LINE&gt; - Defines the secret (client shared secret) up to 64 characters</li></ul> |

### Examples

```
nx9500-6C8809(config-radius-server-policy-test)#nas 172.16.10.10/24 secret 0
nx9500-6C8809(config-radius-server-policy-test)#show context
radius-server-policy test
 authentication eap-auth-type tls
 crl-check
 nas 172.16.10.10/24 secret 0 wirelesswell
 local realm realm1
 ldap-server primary host 172.16.10.19 port 162 login "test" bind-dn "bind-dn1" base-dn
 "base-dn1" passwd 0 test@123 passwd-attr test123 group-attr group1 group-filter
```

```
"groupfilter1" group-membership groupmembership1 net-timeout 2
 ldap-server dead-period 100
nx9500-6C8809(config-radius-server-policy-test)#
```

## Related Commands

|                              |                                                            |
|------------------------------|------------------------------------------------------------|
| <code>no</code> on page 1575 | Removes a RADIUS server's client on a RADIUS server policy |
|------------------------------|------------------------------------------------------------|

### *proxy*

Configures a proxy RADIUS server based on the realm/suffix. The realm identifies where the RADIUS server forwards AAA requests for processing.

A user's access request is sent to a proxy RADIUS server if it cannot be authenticated by the local RADIUS resources. The proxy server checks the information in the user access request and either accepts or rejects the request. If the proxy server accepts the request, it returns configuration information specifying the type of connection service required to authenticate the user.

The RADIUS proxy appears to act as a RADIUS server to NAS, whereas the proxy appears to act as a RADIUS client to the RADIUS server.

When the proxy server receives a request for a user name with a realm, the server references a table of realms. If the realm is known, the server proxies the request to the RADIUS server.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
proxy [realm|retry-count|retry-delay]
proxy realm <REALM-NAME> server <IP> port <1024-65535> secret [0 <PASSWORD>|2 <ENCRYPTED-
PASSWORD>|<PASSWORD>]
proxy retry-count <3-6>
proxy retry-delay <5-10>
```

### Parameters

```
proxy realm <REALM-NAME> server <IP> port <1024-65535> secret [0 <PASSWORD>|2 <ENCRYPTED-
PASSWORD>|<PASSWORD>]
```

|                          |                                                                                                                                                                                                                                                                                                                            |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| proxy realm <REALM-NAME> | <p>Configures the realm name</p> <ul style="list-style-type: none"> <li>• &lt;REALM-NAME&gt; - Specify the realm name. The name should not exceed 50 characters.</li> </ul>                                                                                                                                                |
| server <IP>              | <p>Configures the proxy server's IP address. This is the address of server checking the information in the user access request and either accepting or rejecting the request on behalf of the local RADIUS server.</p> <ul style="list-style-type: none"> <li>• &lt;IP&gt; - Sets the proxy server's IP address</li> </ul> |

|                                                                        |                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| port <1024-65535>                                                      | Configures the proxy server's port. This is the TCP/IP port number for the server that acts as a data source for the proxy server. <ul style="list-style-type: none"> <li>• &lt;1024-65535&gt; - Sets the proxy server's port from 1024 - 65535 (default port is 1812)</li> </ul>                        |
| secret [0<br><PASSWORD>  2<br><ENCRYPTED-<br>PASSWORD>  <br><PASSWORD> | Sets the proxy server secret string. The options are: <ul style="list-style-type: none"> <li>• 0 &lt;PASSWORD&gt; - Sets an UNENCRYPTED password</li> <li>• 2 &lt;ENCRYPTED-PASSWORD&gt; - Sets an ENCRYPTED password</li> <li>• &lt;PASSWORD&gt; - Sets the proxy server shared secret value</li> </ul> |

proxy retry-count <3-6>

|                      |                                                                                                                                                                                                                                                                 |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| retry-count<br><3-6> | Sets the proxy server's retry count. This is the maximum number of attempts made by a controllers RADIUS server to connect to the proxy server. <ul style="list-style-type: none"> <li>• &lt;3-6&gt; - Sets a value from 3 - 6 (default is 3 counts)</li> </ul> |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

proxy retry-delay <5-10>

|                       |                                                                                                                                                                                                                                                                                 |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| retry-delay<br><5-10> | Sets the proxy server's retry delay count. This is the interval the controller's RADIUS server waits before making an additional connection attempt. <ul style="list-style-type: none"> <li>• &lt;5-10&gt; - Sets a value from 5 - 10 seconds (default is 5 seconds)</li> </ul> |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Usage Guidelines

A maximum of five RADIUS proxy servers can be configured. The proxy server attempts six retries before it times out. The retry count defines the number of times RADIUS requests are transmitted before giving up. The timeout value is the defines the interval between successive retransmission of a RADIUS request (in case of no reply).

### Examples

```
nx9500-6C8809(config-radius-server-policy-test)#proxy realm test1 server 172.16.10.7 port
1025 secret 0 test1123
nx9500-6C8809(config-radius-server-policy-test)#proxy retry-count 4
nx9500-6C8809(config-radius-server-policy-test)#proxy retry-delay 8
nx9500-6C8809(config-radius-server-policy-test)#show context
radius-server-policy test
 proxy retry-delay 8
 proxy retry-count 4
 proxy realm test1 server 172.16.10.7 port 1025 secret 0 test1123
 ldap-server primary host 172.16.10.19 port 162 login "test" bind-dn "bind-dn1" base-dn
"bas-dn1" passwd 0 test@123 passwd-attr test123 group-attr group1 group-filter
"groupfilter1" group-membership groupmembershipl net-timeout 2
nx9500-6C8809(config-radius-server-policy-test)#
```

### Related Commands

|                 |                                                      |
|-----------------|------------------------------------------------------|
| no on page 1575 | Removes or resets the RADIUS proxy server's settings |
|-----------------|------------------------------------------------------|

### *session-resumption*

Enables session resumption or fast re-authentication by using cached attributes. This feature controls the volume and duration cached data is maintained by the server policy, upon termination of a server policy session. The availability and quick retrieval of the cached data speeds up session resumption.



This feature is disabled by default.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
session-resumption {lifetime|max-entries}
session-resumption {lifetime <1-24> {max-entries <10-1024>}/max-entries <10-1024>}
```

### Parameters

```
session-resumption {lifetime <1-24> {max-entries <10-1024>}/max-entries <10-1024>}
```

|                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| lifetime <1-24><br>{max-entries<br><10-1024>} | Optional. Sets the lifetime of cached entries <ul style="list-style-type: none"><li>• &lt;1-24&gt; - Specify the lifetime period from 1 - 24 hours (default is 1 hour)</li><li>• max-entries - Optional. Configures the maximum number of entries in the cache<ul style="list-style-type: none"><li>• &lt;10-1024&gt; - Sets the maximum number of entries in the cache from 10 - 1024 (default is 128 entries)</li></ul></li></ul> |
| max-entries<br><10-1024>                      | Optional. Configures the maximum number of entries in the cache <ul style="list-style-type: none"><li>• &lt;10-1024&gt; - Sets the maximum number of entries in the cache from 10 - 1024 (default is 128 entries)</li></ul>                                                                                                                                                                                                         |

### Examples

```
nx9500-6C8809(config-radius-server-policy-test)#session-resumption lifetime 10 max-entries 11
nx9500-6C8809(config-radius-server-policy-test)#show context
radius-server-policy test
 proxy retry-delay 8
 proxy retry-count 4
 proxy realm test1 server 172.16.10.7 port 1025 secret 0 test1123
 ldap-server primary host 172.16.10.19 port 162 login "test" bind-dn "bind-dn1" base-dn "bas-dn1" passwd 0 test@123 passwd-attr test123 group-attr group1 group-filter "groupfilter1" group-membership groupmembershipl net-timeout 2
 session-resumption lifetime 10 max-entries 11
nx9500-6C8809(config-radius-server-policy-test)#
```

### Related Commands

|                              |                                                          |
|------------------------------|----------------------------------------------------------|
| <code>no</code> on page 1575 | Disables session resumption on this RADIUS server policy |
|------------------------------|----------------------------------------------------------|

### termination

Enables EAP termination on this RADIUS server policy. When enabled, EAP authentication is terminated at the controller level. This option is disabled by default.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000

- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

termination

### Parameters

None

### Examples

```
nx9500-6C8809(config-radius-server-policy-test)#termination
nx9500-6C8809(config-radius-server-policy-test)#show context
radius-server-policy test
 termination
 no bypass crl-check
nx9500-6C8809(config-radius-server-policy-test)#
```

### Related Commands

|                 |                                                       |
|-----------------|-------------------------------------------------------|
| no on page 1575 | Disables EAP termination on this RADIUS server policy |
|-----------------|-------------------------------------------------------|

use

Defines settings used with the RADIUS server policy

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
use [radius-group <RAD-GROUP-NAME1> {RAD-GROUP-NAME2}|radius-user-pool-policy <RAD-USER-POOL-NAME>]
```

### Parameters

```
use [radius-group <RAD-GROUP-NAME1> {RAD-GROUP-NAME2}|radius-user-pool-policy <RAD-USER-POOL-NAME>]
```

|                                                  |                                                                                                                                                                    |
|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| radius-group <RAD-GROUP-NAME1> {RAD-GROUP-NAME2} | Associates a specified RADIUS group (for LDAP users) with this RADIUS server policy. You can optionally associate two RADIUS groups with one RADIUS server policy. |
| radius-user-pool-policy <RAD-USER-POOL-NAME>     | Associates a specified RADIUS user pool with this RADIUS server policy. Specify a user pool name.                                                                  |

### Examples

```
nx9500-6C8809(config-radius-server-policy-test)#use radius-group test
nx9500-6C8809(config-radius-server-policy-test)#show context
radius-server-policy test
 proxy retry-delay 8
 proxy retry-count 4
 proxy realm test1 server 172.16.10.7 port 1025 secret 0 test1123
 ldap-server primary host 172.16.10.19 port 162 login "test" bind-dn "bind-dn1" base-dn
```

```
"bas-dn1" passwd 0 test@123 passwd-attr test123 group-attr group1 group-filter
"groupfilter1" group-membership groupmembershipl net-timeout 2
 use radius-group test
 session-resumption lifetime 10 max-entries 11
nx9500-6C8809(config-radius-server-policy-test)#
```

## Related Commands

`no` on page 1575 Disassociates a RADIUS group or a RADIUS user pool policy from this RADIUS server policy

*no*

Negates a command or reverts back to default settings. When used with in the config RADIUS server policy mode, the `no` command removes settings, such as `crl-check`, LDAP group verification, RADIUS client, etc.

## Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
no [authentication|bypass|chase-referral|crl-check|ldap-agent|ldap-group-verification|
ldap-server|local|nas|proxy|session-resumption|termination|use]
no bypass [crl-check|expired-crl]
no authentication [data-source|eap]
no authentication [data-source {ldap {fallback}|local|ssid}|eap configuration]
no [chase-referral|crl-check|ldap-group-verification|nas <IP/M>|session-resumption]
no ldap-agent [join-retry-timeout|primary|secondary]
no local realm [<REALM-NAME>|all]
no proxy [realm <REALM-NAME>|retry-count|retry-delay]
no ldap-server [dead-period|primary|secondary]
no termination
no use [radius-group [<RAD-GROUP-NAME>|all]|radius-user-pool-policy [<RAD-USER-POOL-NAME>|
all]]
```

## Parameters

`no` <PARAMETERS>

`no` <PARAMETERS> Negates a command or reverts back to default settings. When used with in the config RADIUS server policy mode, the `no` command removes settings, such as `crl-check`, LDAP group verification, RADIUS client, etc.

## Examples

The following example shows the RADIUS server policy 'test' settings before the 'no' commands are executed:

```
nx9500-6C8809(config-radius-server-policy-test)#show context
radius-server-policy test
 authentication eap-auth-type tls
 crl-check
 nas 172.16.10.10/24 secret 0 wirelesswell
 local realm realm1
 ldap-server primary host 172.16.10.19 port 162 login "test" bind-dn "bind-dn1" base-dn
"bas-dn1" passwd 0 test@123 passwd-attr test123 group-attr group1 group-filter
```

```

"groupfilter1" group-membership groupmembership1 net-timeout 2
 ldap-server dead-period 100
nx9500-6C8809(config-radius-server-policy-test)#
nx9500-6C8809(config-radius-server-policy-test)#no authentication eap configuration
nx9500-6C8809(config-radius-server-policy-test)#no curl-check
nx9500-6C8809(config-radius-server-policy-test)#no local realm realm1
nx9500-6C8809(config-radius-server-policy-test)#no nas 172.16.10.10/24
nx9500-6C8809(config-radius-server-policy-test)#no ldap-server dead-period

```

The following example shows the RADIUS server policy 'test' settings after the 'no' commands are executed:

```

nx9500-6C8809(config-radius-server-policy-test)#show context
radius-server-policy test
 ldap-server primary host 172.16.10.19 port 162 login "test" bind-dn "bind-dn1" base-dn
"bas-dn1" passwd 0 test@123 passwd-attr test123 group-attr group1 group-filter
"groupfilter1" group-membership groupmembership1 net-timeout 2
nx9500-6C8809(config-radius-server-policy-test)#

```

## radius-user-pool-policy

Configures a RADIUS user pool policy and enters its configuration mode

A user pool defines policies for individual user access to the internal RADIUS resources. User pool policies define unique permissions (either temporary or permanent) that control user access to the local RADIUS resources. A pool can contain a single user or multiple users.

Use the (config) instance to configure RADIUS user pool policy commands. To navigate to the radius-user-pool-policy instance, use the following commands:

```

<DEVICE>(config)#radius-user-pool-policy <POOL-NAME>
nx9500-6C8809(config)#radius-user-pool-policy testuser
nx9500-6C8809(config-radius-user-pool-testuser)#?
Radius User Pool Mode commands:
 duration Set a guest user's access duration
 no Negate a command or set its defaults
 user Radius user configuration

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-radius-user-pool-testuser)#

```

The following table summarizes RADIUS user pool policy configuration commands.

Table: RADIUS-User-Pool Config Mode Commands

| Commands                           | Description                                               |
|------------------------------------|-----------------------------------------------------------|
| <code>duration</code> on page 1577 | Modifies a guest user's duration of captive-portal access |
| <code>user</code> on page 1577     | Configures the RADIUS user parameters                     |
| <code>no</code> on page 1580       | Negates a command or sets its default                     |

### *duration*

Modifies the duration, in minutes, that a guest user can access the captive portal

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
duration <GUEST-USER-NAME> <0-525600>
```

#### Parameters

```
duration <GUEST-USER-NAME> <0-525600>
```

|                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>duration &lt;GUEST-USER-NAME&gt; &lt;0-525600&gt;</pre> | <p>Modifies the duration of captive-portal access (in minutes) for the guest user identified by the &lt;GUEST-USER-NAME&gt; keyword</p> <ul style="list-style-type: none"> <li>• &lt;GUEST-USER-NAME&gt; - Specify the guest user's name.</li> <li>• &lt;0-525600&gt; - Specify the access duration from 0 - 525600 minutes. A value of "0" indicates unlimited access. The default is 1440 minutes.</li> </ul> |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
rfs4000-229D58(config-radius-user-pool-wdws)#show context
radius-user-pool-policy wdws
 user guestuser1 password 0 guestuser@1 group wdws guest expiry-time 12:30 expiry-date
12/15/2014 access-duration 500
rfs4000-229D58(config-radius-user-pool-wdws)#
rfs4000-229D58(config-radius-user-pool-wdws)#duration guestuser1 200
rfs4000-229D58(config-radius-user-pool-wdws)#show context
radius-user-pool-policy wdws
 user guestuser1 password 0 guestuser@1 group wdws guest expiry-time 12:30 expiry-date
12/15/2014 access-duration 200
rfs4000-229D58(config-radius-user-pool-wdws)#
```

### *user*

Configures RADIUS user parameters

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000

- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```

user <USERNAME> password [0 <UNENCRYPTED-PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>]
{group <RAD-GROUP-NAME>} {guest}
user <USERNAME> password [0 <UNENCRYPTED-PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>]
{group <RAD-GROUP-NAME>} {guest expiry-time <HH:MM> expiry-date <MM/DD/YYYY>
{access-duration <0-525600>|data-limit|email-id <EMAIL-ID>|start-time <HH:MM> start-date
<MM/DD/YYY>|
telephone <TELEPHONE-NUMBER>}}
user <USERNAME> password [0 <UNENCRYPTED-PASSWORD>|2 <ENCRYPTED-PASSWORD>|
<PASSWORD>] {group <RAD-GROUP-NAME>} {guest expiry-time <HH:MM> expiry-date <MM/DD/YYYY>
{access-duration <0-525600>|data-limit <1-102400> committed-downlink <100-1000000>
committed-uplink <100-1000000> reduced-downlink <100-1000000> reduced-uplink <100-1000000>|
email-id <EMAIL-ID>|start-time <HH:MM> start-date <MM/DD/YYY>|telephone <TELEPHONE-
NUMBER>}}

```

## Parameters

```

user <USERNAME> password [0 <UNENCRYPTED-PASSWORD>|2 <ENCRYPTED-PASSWORD>|
<PASSWORD>] {group <RAD-GROUP-NAME>} {guest expiry-time <HH:MM> expiry-date <MM/DD/YYYY>
{access-duration <0-525600>|data-limit <1-102400> committed-downlink <100-1000000>
committed-uplink <100-1000000> reduced-downlink <100-1000000> reduced-uplink <100-1000000>|
email-id <EMAIL-ID>|start-time <HH:MM> start-date <MM/DD/YYY>|telephone <TELEPHONE-
NUMBER>}}

```

|                                                                     |                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| user <USERNAME>                                                     | <p>Adds a new RADIUS user to the RADIUS user pool</p> <ul style="list-style-type: none"> <li>• &lt;USERNAME&gt; – Specify the name of the user. The username should not exceed 64 characters.</li> </ul> <p><b>Note:</b> The username is a unique alphanumeric string identifying this user, and cannot be modified with the rest of the configuration.</p>   |
| passwd [0 <UNENCRYPTED-PASSWORD> 2 <ENCRYPTED-PASSWORD> <PASSWORD>] | <p>Configures the user password (provide a password unique to this user)</p> <ul style="list-style-type: none"> <li>• 0 &lt;UNENCRYPTED-PASSWORD&gt; – Sets an unencrypted password</li> <li>• 2 &lt;ENCRYPTED-PASSWORD&gt; – Sets an encrypted password</li> <li>• &lt;PASSWORD&gt; – Sets a password (specified unencrypted) up to 21 characters</li> </ul> |
| group <RAD-GROUP-NAME>                                              | <p>Optional. Configures the RADIUS server group of which this user is a member</p> <ul style="list-style-type: none"> <li>• &lt;RAD-GROUP-NAME&gt; – Specify the group name in the local database.</li> </ul> <p><b>Note:</b> If the user is a guest, assign the user a group with temporary access privileges.</p>                                           |
| guest                                                               | <p>Optional. Specifies that this user is a guest user. Guest users have restricted access. After enabling a guest user account, specify the expiry time and date for this account.</p> <p>A guest user can be assigned only to a guest user group.</p>                                                                                                        |
| expiry-time <HH:MM>                                                 | <p>Specify the user account expiry time in the HH:MM format (for example, 12:30 means 30 minutes after 12:00 the user login will expire).</p>                                                                                                                                                                                                                 |
| expiry-date <MM:DD:YYYY>                                            | <p>Specify the user account expiry date in the MM:DD:YYYY format (for example, 02:15:2014).</p>                                                                                                                                                                                                                                                               |

|                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| start-time <HH:MM>                                                                                                                                                                                                                                                                                                                                    | Optional. Specify the user account activation time in the HH:MM format.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <pre>{access-duration &lt;0-525600&gt; data-limit &lt;1-102400&gt; committed- downlink &lt;100-1000000&gt; committed-uplink &lt;100-1000000&gt; reduced- downlink &lt;100-1000000&gt; reduced-uplink &lt;100-1000000&gt;  email-id &lt;EMAIL-ID&gt;  start-time &lt;HH:MM&gt; start-date &lt;MM:DD:YYY&gt;  telephone &lt;TELEPHONE-NUMBER&gt;}</pre> | <p>After configuring the above user details, optionally configure the following user information:</p> <ul style="list-style-type: none"> <li>• access-duration &lt;0-525600&gt; – Configures the duration, in minutes, for which this guest user can access the captive portal. <ul style="list-style-type: none"> <li>• &lt;0-525600&gt; – Specify a value from 0 - 525600 minutes.</li> </ul> </li> <li>• data-limit &lt;1-102400&gt; – Configures the data limit for which this guest user can access the captive portal. Specify a value from 1 - 102400 bytes.</li> <li>• committed-downlink &lt;100-1000000&gt; – Configures committed download bandwidth until data limit is reached. This value represents the download speed (in kilobits per second) allocated to the guest user. When bandwidth is available, the user can download data at the specified rate. If a guest user has a bandwidth based policy and exceeds the specified data limit, the speed is throttled to the reduced download rate (specified using this command). Specify a value from 100 - 1000000 Kbps. <ul style="list-style-type: none"> <li>committed-uplink &lt;100-1000000&gt; – Configures committed uplink bandwidth until data limit is reached. This value represents the upload speed (in kilobits per second) allocated to the guest user. When bandwidth is available, the user can upload data at the specified rate. If a guest user has a bandwidth based policy and exceeds the specified data limit, the speed is throttled to the reduced uplink rate (specified using this command). Specify a value from 100 - 1000000 Kbps.</li> <li>reduced-downlink &lt;100-1000000&gt; – Configures reduced download bandwidth after data Limit is reached. This value represents the reduced speed the guest utilizes (in kilobits per second) when exceeding the specified data limit, if applicable. If a guest user has a bandwidth based policy and exceeds the specified data limit, the speed is throttled to the reduced download rate specified here. Specify a value from 100-1000000 Kbps.</li> <li>reduced-uplink &lt;100-1000000&gt; – Configures reduced uplink bandwidth after data Limit is reached. This value represents the reduced speed the guest utilizes (in kilobits per second) when exceeding the specified data limit, if applicable. If a guest user has a bandwidth based policy and exceeds the specified data limit, the speed is throttled to the reduced uplink rate specified here. Specify a value from 100 - 1000000 Kbps.</li> </ul> </li> </ul> <ul style="list-style-type: none"> <li>• email-id – Optional. User’s e-mail ID</li> <li>• start-time – Optional. User’s account activation time. After specifying the activation time, specify the activation date. <ul style="list-style-type: none"> <li>• start-date – User’s account activation date</li> </ul> </li> <li>• telephone – Optional. User’s telephone number (should include the area code)</li> </ul> <p>To view access details of guest users on a RADIUS server, in the PriviExecutable Configuration mode, use the following command:</p> <pre>show &gt; radius &gt; guest-users nx9500-6C8809#show radius guest-users time           TIME (min:sec)         USED   REMAINING  GUEST USER         0:00     500:00   user1 Current time: 09:03:07 nx9500-6C8809#</pre> |

## Examples

```
rfs4000-229D58(config-radius-user-pool-wdws)#user guestuser1 password 0 guestuser@1
group wdws guest expiry-time 12:30 expiry-date 12/15/2014 access-duration 500
rfs4000-229D58(config-radius-user-pool-wdws)#show context
radius-user-pool-policy wdws
 user guestuser1 password 0 guestuser@1 group wdws guest expiry-time 12:30 expiry-date
 12/15/2014 access-duration 500
rfs4000-229D58(config-radius-user-pool-wdws)#
```

## Related Commands

|                              |                                        |
|------------------------------|----------------------------------------|
| <code>no</code> on page 1580 | Deletes a user from a RADIUS user pool |
|------------------------------|----------------------------------------|

*no*

Negates a command or sets its default. When used in the RADIUS user pool policy mode, the `no` command deletes a user from a RADIUS user pool

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
no user <USERNAME>
```

## Parameters

```
no user <USERNAME>
```

|                                       |                                                                                                                                |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <code>no user &lt;USERNAME&gt;</code> | Deletes a RADIUS user <ul style="list-style-type: none"><li>• <code>&lt;USERNAME&gt;</code> - Specify the user name.</li></ul> |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|

## Examples

The following example shows the RADIUS user pool 'testuser' settings before the 'no' command is executed:

```
rfs4000-229D58(config-radius-user-pool-wdws)#show context
radius-user-pool-policy wdws
 user guestuser1 password 0 guestuser@1 group wdws guest expiry-time 12:30 expiry-date
 12/15/2014 access-duration 500
rfs4000-229D58(config-radius-user-pool-wdws)#
rfs4000-229D58(config-radius-user-pool-wdws)#no user guestuser1
```

The following example shows the RADIUS user pool 'testuser' settings after the 'no' command is executed:

```
rfs4000-229D58(config-radius-user-pool-wdws)#show context
radius-user-pool-policy wdws
rfs4000-229D58(config-radius-user-pool-wdws)#
```



# RADIO QoS POLICY

## RADIO-QOS-POLICY

---

This chapter summarizes the radio QoS policy in the CLI command structure.

Configuring and implementing a radio QoS policy is essential for WLANs with heavy traffic and less bandwidth. The policy enables you to provide preferential service to selected network traffic by controlling bandwidth allocation. The radio QoS policy can be applied to VLANs configured on an access point. In case no VLANs are configured, the radio QoS policy can be applied to an access point's Ethernet and radio ports.

Without a dedicated QoS policy, a network operates on a best-effort delivery basis, meaning all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped!

When configuring a Radio QoS policy, select specific network traffic, prioritize it, and use congestion-management and congestion-avoidance techniques to provide deployment customizations best suited to each QoS policy's intended wireless client base.

A well designed QoS policy should:

- Classify and mark data traffic to accurately prioritize and segregate it (by access category) throughout the network.
- Minimize network delay and jitter for latency sensitive traffic.
- Ensure higher priority traffic has a better likelihood of delivery in the event of network congestion.
- Prevent ineffective utilization of access points degrading session quality by configuring admission control mechanisms within each radio QoS policy.

Within a managed wireless network, wireless clients supporting low and high priority traffic contend with one another for access and data resources. The IEEE 802.11e amendment has defined EDCA (Enhanced Distributed Channel Access) mechanisms stating high priority traffic can access the network sooner than lower priority traffic. The EDCA defines four traffic classes (or access categories); voice (highest), video (next highest), best effort, and background (lowest). The EDCA has defined a time interval for each traffic class, known as the TXOP (Transmit Opportunity). The TXOP prevents traffic of a higher priority from completely dominating the wireless medium, thus ensuring lower priority traffic is still supported.

IEEE 802.11e includes an advanced power saving technique called U-APSD (Unscheduled Automatic Power Save Delivery) that provides a mechanism for wireless clients to retrieve packets buffered by an access point. U-APSD reduces the amount of signaling frames sent from a client to retrieve buffered data from an access point. U-APSD also allows access points to deliver buffered data frames as bursts, without backing-off between data frames. These improvements are useful for voice clients, as they provide improved battery life and call quality.

The Wi-Fi alliance has created WMM (Wireless Multimedia) and WMM-PS (WMM Power Save) certification programs to ensure interoperability between 802.11e WLAN infrastructure implementations

and wireless clients. A wireless network supports both WMM and WMM-Power Save techniques. WMM and WMM-PS (U-APSD) are enabled by default in each WLAN profile.

Enabling WMM support on a WLAN just advertises the WLAN's WMM capability and radio configuration to wireless clients. The wireless clients must also support WMM and use the values correctly while accessing the WLAN to benefit.

WMM includes advanced parameters (CWMin, CWMax, AIFSN and TXOP) specifying back-off duration and inter-frame spacing when accessing the network. These parameters are relevant to both connected access point radios and their wireless clients. Parameters impacting access point transmissions to their clients are controlled using per radio WMM settings, while parameters used by wireless clients are controlled by a WLAN's WMM settings.

Wireless network controllers (access points, controllers, and service platforms) include a SIP (Session Initiation Protocol), SCCP (Skinny Call Control Protocol) and ALG (Application Layer Gateway) enabling devices to identify voice streams and dynamically set voice call bandwidth.

Wireless network controllers also support static QoS mechanisms per WLAN to provide prioritization of WLAN traffic when legacy (non WMM) clients are deployed. When enabled on a WLAN, traffic forwarded to a client is prioritized and forwarded based on the WLAN's WMM access control setting.



#### Note

Statically setting a WLAN WMM access category value only prioritizes traffic to the client.

Wireless network administrators can also assign weights to each WLAN in relation to user priority levels. The lower the weight, the lower the priority. Use a weighted technique to achieve different QoS levels across WLANs.

All devices rate-limit bandwidth for WLAN sessions. This form of per-user rate limiting enables administrators to define uplink and downlink bandwidth limits for users and clients. This sets the level of traffic a user or client can forward and receive over the WLAN. If the user or client exceeds the limit, excessive traffic is dropped.

Rate limits can be applied to WLANs using groups defined locally or externally from a RADIUS server using VSAs (Vendor Specific Attributes). Rate limits can be applied to users authenticating using 802.1X, captive portal authentication, and devices using MAC authentication.

Use the (config) instance to configure radios QoS policy related configuration commands. To navigate to the radio QoS policy instance, use the following commands:

```
<DEVICE>(config)#radio-qos-policy <POLICY-NAME>
nx9500-6C8809(config)#radio-qos-policy test
nx9500-6C8809(config-radio-qos-test)#?
Radio QoS Mode commands:
 accelerated-multicast Configure multicast streams for acceleration
 admission-control Configure admission-control on this radio for one or
 more access categories
 no Negate a command or set its defaults
 smart-aggregation Configure smart aggregation parameters
 wmm Configure 802.11e/Wireless MultiMedia parameters

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
```

```

exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

```

```
nx9500-6C8809(config-radio-qos-test)#
```

## radio-qos-policy-commands

The following table summarizes radio QoS policy configuration commands:

**Table 48: Radio-QoS-Policy Config Mode Commands**

| Command                                            | Description                                                                   |
|----------------------------------------------------|-------------------------------------------------------------------------------|
| <a href="#">accelerated-multicast</a> on page 1583 | Configures multicast streams for acceleration                                 |
| <a href="#">admission-control</a> on page 1584     | Enables admission control across all radios for one or more access categories |
| <a href="#">smart-aggregation</a> on page 1588     | Configures smart aggregation parameters                                       |
| <a href="#">service</a> on page 1589               | Invokes service commands in the radio QoS configuration mode                  |
| <a href="#">wmm</a> on page 1590                   | Configures 802.11e/wireless multimedia parameters                             |
| <a href="#">no</a> on page 1592                    | Negates a command or resets configured settings to their default              |



### Note

For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see [COMMON COMMANDS](#) on page 640.



### Note

The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (\_) character. In other words, the name of a device cannot contain an underscore.

### *accelerated-multicast*

Configures multicast streams for acceleration. Multicasting allows group transmission of data streams.

#### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
accelerated-multicast [client-timeout|max-client-streams|max-streams|overflow-policy|
stream-threshold]
accelerated-multicast [client-timeout <5-6000>|max-client-streams <1-4>|max-streams
<0-256>|
overflow-policy [reject|revert]|stream-threshold <1-500>]
```

## Parameters

```
accelerated-multicast [client-timeout <5-6000>|max-client-streams <1-4>|max-streams
<0-256>|
overflow-policy [reject|revert]|stream-threshold <1-500>]
```

|                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| client-timeout<br><5-6000>>        | Configures a timeout period in seconds for wireless clients <ul style="list-style-type: none"><li>&lt;5-6000&gt; - Specify a value from 5 - 6000 seconds. The default is 60 seconds.</li></ul>                                                                                                                                                                                                                                                                                                                                                                  |
| max-client-streams<br><1-4>        | Configures the maximum number of accelerated multicast streams per client <ul style="list-style-type: none"><li>&lt;1-4&gt; - Specify a value from 1 - 4. The default is 2.</li></ul>                                                                                                                                                                                                                                                                                                                                                                           |
| max-streams<br><0-256>             | Configures the maximum number of accelerated multicast streams per radio <ul style="list-style-type: none"><li>&lt;0-256&gt; - Specify a value from 0 - 256. The default is 25.</li></ul>                                                                                                                                                                                                                                                                                                                                                                       |
| overflow-policy<br>[reject revert] | Specifies the policy in case too many clients register simultaneously. The radio QoS policy can be configured to follow one of the following courses of action: <ul style="list-style-type: none"><li>reject - Rejects new clients. The default overflow policy is reject.</li><li>revert - Reverts to regular multicast delivery</li></ul> When the number of wireless clients using accelerated multicast exceeds the configured value (max-streams), the radio can either reject new wireless clients or revert existing clients to a non-accelerated state. |
| stream-threshold<br><1-500>        | Configures the number of multicast packets per second threshold value. Once this threshold is crossed, the system triggers streams to accelerate. <ul style="list-style-type: none"><li>&lt;1-500&gt; - Specify a value from 1 - 500. The default is 25 packets per second.</li></ul>                                                                                                                                                                                                                                                                           |

## Examples

```
nx9500-6C8809(config-radio-qos-test)#accelerated-multicast client-timeout 500
nx9500-6C8809(config-radio-qos-test)#accelerated-multicast stream-threshold 15
nx9500-6C8809(config-radio-qos-test)#show context
radio-qos-policy test
 accelerated-multicast stream-threshold 15
 accelerated-multicast client-timeout 500
nx9500-6C8809(config-radio-qos-test)#
```

## Related Commands

|                 |                                                            |
|-----------------|------------------------------------------------------------|
| no on page 1592 | Reverts accelerated multicasting settings to their default |
|-----------------|------------------------------------------------------------|

### *admission-control*

Enables admission control across all radios for one or more access categories. Enabling admission control for an access category ensures clients associated to an access point complete WMM admission control before using that access category.

## Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
admission-control [background|best-effort|firewall-detected-traffic|implicit-tspec|
video|voice]
admission-control [firewall-detected-traffic|implicit-tspec]
admission-control [background|best-effort|video|voice]
{max-airtime-percent|max-clients|max-roamed-clients|reserved-for-roam-percent}
admission-control [background|best-effort|video|voice] {max-airtime-percent <0-150>/
max-clients <0-256>/max-roamed-clients <0-256>/reserved-for-roam-percent <0-150>}
```

## Parameters

```
admission-control [firewall-detected-traffic|implicit-tspec]
```

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| admission-control firewall-detected-traffic | Enforces admission control for traffic whose access category is detected by the firewall ALG. For example, SIP voice calls. This feature is enabled by default. When enabled, the firewall simulates reception of frames for voice traffic when the voice traffic was originated via SIP or SCCP control traffic. If a client exceeds configured values, the call is stopped and/or received voice frames are forwarded at the next non admission controlled traffic class priority. This applies to clients that do not send TPSEC frames only.                                                                                                                                                                                                                                                               |
| admission-control implicit-tspec            | Enables implicit traffic specifiers for clients that do not support WMM TSPEC, but are accessing admission-controlled access categories. This feature is enabled by default. This feature requires wireless clients to send their traffic specifications to an access point before they can transmit or receive data. If enabled, this setting applies to this radio QoS policy. When enabled, the access point simulates the reception of frames for any traffic class by looking at the amount of traffic the client is receiving and sending. If the client sends more traffic than has been configured for an admission controlled traffic class, the traffic is forwarded at the priority of the next non admission controlled traffic class. This applies to clients that do not send TPSEC frames only. |

```
admission-control [background|best-effort|video|voice]
{max-airtime-percent|max-clients|max-roamed-clients|reserved-for-roam-percent}
```

|                               |                                                                     |
|-------------------------------|---------------------------------------------------------------------|
| admission-control background  | Configures background access category admission control parameters  |
| admission-control best-effort | Configures best effort access category admission control parameters |
| admission-control video       | Configures video access category admission control parameters       |
| admission-control voice       | Configures voice access category admission control parameters       |

|                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>max-airtime-percent<br/>&lt;0-150&gt;</p> | <p>Optional. Specifies the maximum percentage of airtime, including over subscription, for the following access category:</p> <ul style="list-style-type: none"> <li>• background – Sets the maximum airtime (in the form of a percentage of the radio’s bandwidth) allotted to admission control for low (background) client traffic. Background traffic only needs a short radio airtime to process, so set an intermediate airtime value if this radio QoS policy is reserved to support background data.</li> <li>• best-effort – Sets the maximum airtime (in the form of a percentage of the radio’s bandwidth) allotted to admission control for normal (best-effort) client traffic. Normal best effort traffic needs a short radio airtime to process, so set an intermediate airtime value if this radio QoS policy is reserved for best effort data support.</li> <li>• video – Sets the maximum airtime (in the form of a percentage of the radio’s bandwidth) allotted to admission control for voice supported client traffic. Video traffic requires longer radio airtime to process, so set a longer airtime value if this radio QoS policy is intended to support video.</li> <li>• voice – Sets the maximum airtime (in the form of a percentage of the radio’s bandwidth) allotted to admission control for voice supported client traffic. Voice traffic requires longer radio airtime to process, so set a longer airtime value if this radio QoS policy is intended to support voice.</li> </ul> <p>The following keyword is common to all of the above traffic types:</p> <ul style="list-style-type: none"> <li>• &lt;0-150&gt; – Specify a value from 0 - 150. This is the maximum percentage of airtime, including over subscription, for the selected access category. The default is 75%.</li> </ul> |
| <p>max-clients &lt;0-256&gt;</p>             | <p>Optional. Specifies the maximum number of wireless clients admitted to the following access categories:</p> <ul style="list-style-type: none"> <li>• background – Sets the number of wireless clients supporting low (background) traffic allowed to exist (and consume bandwidth) within the radio’s QoS policy</li> <li>• best-effort – Sets the number of wireless clients supporting normal (best-effort) traffic allowed to exist (and consume bandwidth) within the radio’s QoS policy</li> <li>• video – Sets the number of video supported wireless clients allowed to exist (and consume bandwidth) within the radio’s QoS policy.</li> <li>• voice – Sets the number of voice supported wireless clients allowed to exist (and consume bandwidth) within the radio’s QoS policy.</li> </ul> <p>Since voice and video supported wireless clients use a greater portion of a controller’s resources than lower bandwidth traffic (like low and best effort categories), consider setting the max-client value proportionally to the number of other QoS policies supporting voice access category clients.</p> <p>The following keyword is common to all of the above traffic types:</p> <ul style="list-style-type: none"> <li>• &lt;0-256&gt; – Specify a value from 0 - 256. This is the maximum number of wireless clients admitted to the selected access category. The default is 100 clients.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                       |

|                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>max-roamed-clients<br/>&lt;0-256&gt;</p>        | <p>Optional. Specifies the maximum number of roaming wireless clients admitted to the selected access category</p> <ul style="list-style-type: none"> <li>• background – Sets the number of low (background) supported wireless clients allowed to roam to a different access point radio</li> <li>• best-effort – Sets the number of normal (best-effort) supported wireless clients allowed to roam to a different access point radio</li> <li>• video – Sets the number of video supported wireless clients allowed to roam to a different access point radio</li> <li>• voice – Sets the number of voice supported wireless clients allowed to roam to a different access point radio</li> </ul> <p>The following keyword is common to all of the above traffic types:</p> <ul style="list-style-type: none"> <li>• &lt;0-256&gt; – Specify a value from 0 - 256. This is the maximum number of roaming wireless clients admitted to the selected access category. The default is 10 roamed clients.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <p>reserved-for-roam-percent<br/>&lt;0-150&gt;</p> | <p>Optional. Calculates the percentage of air time, including over subscription, allocated exclusively for roaming clients. This value is calculated relative to the configured max air time for this access category.</p> <ul style="list-style-type: none"> <li>• background – Sets the roam utilization (in the form of a percentage of the radio's bandwidth) allotted to admission control for low (background) supported clients who have roamed to a different radio.</li> <li>• best-effort – Sets the roam utilization (in the form of a percentage of the radio's bandwidth) allotted to admission control for normal (best-effort) supported clients who have roamed to a different radio.</li> <li>• video – Sets the roam utilization (in the form of a percentage of the radio's bandwidth) allotted to admission control for video supported clients who have roamed to a different radio.</li> <li>• voice – Sets the roam utilization (in the form of a percentage of the radio's bandwidth) allotted to admission control for voice supported clients who have roamed to a different radio.</li> </ul> <p>The following keyword is common to all of the above traffic types:</p> <ul style="list-style-type: none"> <li>• &lt;0-150&gt; – Specify a value from 0 - 150. This is the percentage of air time, including over subscription, allocated exclusively for roaming clients associated with the selected access category. The default is 10%.</li> </ul> |

## Examples

```

nx9500-6C8809(config-radio-qos-test)#admission-control best-effort max-clients 200
nx9500-6C8809(config-radio-qos-test)#admission-control voice reserved-for-roam-percent 8
nx9500-6C8809(config-radio-qos-test)#admission-control voice max-airtime-percent 9
nx9500-6C8809(config-radio-qos-test)#show context
radio-qos-policy test
admission-control voice max-airtime-percent 9
admission-control voice reserved-for-roam-percent 8
admission-control best-effort max-clients 200
accelerated-multicast stream-threshold 15
accelerated-multicast client-timeout 500
nx9500-6C8809(config-radio-qos-test)#

```

## Related Commands

|                               |                                                                      |
|-------------------------------|----------------------------------------------------------------------|
| <p><b>no</b> on page 1592</p> | <p>Reverts or resets admission control settings to their default</p> |
|-------------------------------|----------------------------------------------------------------------|

## smart-aggregation

Configures smart aggregation parameters on this Radio QoS policy. Smart aggregation enhances frame aggregation by dynamically selecting the time when the aggregated frame is transmitted. In a frame's typical aggregation, an aggregated frame is sent when:

- A pre-configured number of aggregated frames is reached
- An administrator-defined interval has elapsed since the first frame (of a set of frames to be aggregated) was received
- An administrator-defined interval has elapsed since the last frame (not necessarily the final frame) of a set of frames to be aggregated was received

With this enhancement, an aggregation delay is set uniquely for each traffic class. For example, voice traffic might not be aggregated, but sent immediately. Whereas, background data traffic is set a delay for aggregating frames, and these aggregated frames are sent.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
smart-aggregation {delay|max-mesh-hops|min-aggregation-limit}
smart-aggregation {delay [background|best-effort|streaming-video|video-conferencing|
voice] <0-1000>}
smart-aggregation {max-mesh-hops <1-10>}
smart-aggregation {min-aggregation-limit <0-64>}
```

### Parameters

```
smart-aggregation {delay [background|best-effort|streaming-video|video-conferencing|
voice] <0-1000>}
```

|                    |                                                                                                                                                                      |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| delay              | Optional. Configures the maximum delay parameter for each traffic type. This is the maximum delay, in milliseconds, in the transmission of the first frame received. |
| background         | Configures the maximum delay parameter, in milliseconds, for background traffic (250 msec)                                                                           |
| best-effort        | Configures the maximum delay parameter, in milliseconds, for best effort traffic (150 msec)                                                                          |
| streaming-video    | Configures the maximum delay parameter, in milliseconds, for streaming video traffic (150 msec)                                                                      |
| video-conferencing | Configures the maximum delay parameter, in milliseconds, for video conference traffic (40 msec)                                                                      |
| voice              | Configures the maximum delay parameter, in milliseconds, for voice traffic (0 msec)                                                                                  |
| <0-1000>           | This parameter is common to all of the above traffic types. <ul style="list-style-type: none"><li>• &lt;0-1000&gt; – Specify a value from 0 - 1000 msec.</li></ul>   |

```
smart-aggregation {max-mesh-hops <1-10>}
```



|                      |                                                                                                                                                                                                            |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| max-mesh-hops <1-10> | Optional. Sets the maximum number of expected hops to the destination within a mesh <ul style="list-style-type: none"> <li>• &lt;1-10&gt; – Specify a value from 1 - 10. The default is 3 hops.</li> </ul> |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

smart-aggregation {min-aggregation-limit <0-64>}

|                              |                                                                                                                                                                                                               |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| min-aggregation-limit <0-64> | Optional. Sets the minimum number of aggregates buffered before an aggregate is sent <ul style="list-style-type: none"> <li>• &lt;0-64&gt; – Specify a value from 0 - 64. The default is 8 frames.</li> </ul> |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Examples**

```

nx9500-6C8809(config-radio-qos-test)#smart-aggregation delay voice 50
nx9500-6C8809(config-radio-qos-test)#smart-aggregation delay background 100
nx9500-6C8809(config-radio-qos-test)#show context
radio-qos-policy test
 smart-aggregation delay voice 50
 smart-aggregation delay background 100
nx9500-6C8809(config-radio-qos-test)#

```

**Related Commands**

|                 |                                      |
|-----------------|--------------------------------------|
| no on page 1592 | Resets the minimum aggregation limit |
|-----------------|--------------------------------------|

*service*

Invokes service commands in the radio QoS configuration mode

**Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

**Syntax**

```

service [admission-control|show]
service admission-control across-reassoc
service show cli

```

**Parameters**

```
service admission-control across-reassoc
```

|                                  |                                                                                                                                                                                               |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| service                          | Invokes service commands                                                                                                                                                                      |
| admission-control across-reassoc | Retains previously negotiated TSPEC parameters across re-associations on the radio. For more information on admission-control parameters, see <a href="#">admission-control</a> on page 1584. |

```
service show cli
```

|                  |                                                                                                                                      |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| service show cli | Displays running system information <ul style="list-style-type: none"> <li>• cli – Displays the Radio QoS mode's CLI tree</li> </ul> |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------|



## Examples

```
rfs4000-229D58(config-radio-qos-test)#service admission-control across-reassoc
rfs4000-229D58(config-radio-qos-test)#show context
radio-qos-policy test
 service admission-control across-reassoc
rfs4000-229D58(config-radio-qos-test)#
rfs4000-229D58(config-radio-qos-test)#service show cli
Radio QoS Mode mode:
+-help [help]
 +-search
 +-WORD [help search WORD (|detailed|only-show|skip-show|skip-no)]
 +-detailed [help search WORD (|detailed|only-show|skip-show|skip-no)]
 +-only-show [help search WORD (|detailed|only-show|skip-show|skip-no)]
 +-skip-show [help search WORD (|detailed|only-show|skip-show|skip-no)]
 +-skip-no [help search WORD (|detailed|only-show|skip-show|skip-no)]
+-show
 +-commands [show commands]
 +-adoption
 +-log

--More--]
```

## Related Commands

|                              |                                                                                                  |
|------------------------------|--------------------------------------------------------------------------------------------------|
| <code>no</code> on page 1592 | Disables retention of previously negotiated TSPEC parameters across re-associations on the radio |
|------------------------------|--------------------------------------------------------------------------------------------------|

## wmm

Configures 802.11e WMM (wireless multi media) parameters

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
wmm [background|best-effort|video|voice]
wmm [background|best-effort|video|voice] [aifsn <1-15>|cw-max <0-15>|cw-min <0-15>|
txop-limit <0-65535>]
```

### Parameters

```
wmm [background|best-effort|video|voice] [aifsn <1-15>|cw-max <0-15>|cw-min <0-15>|
txop-limit <0-65535>]
```

|                     |                                                                     |
|---------------------|---------------------------------------------------------------------|
| wmm<br>background   | Configures background access category wireless multimedia settings  |
| wmm best-<br>effort | Configures best effort access category wireless multimedia settings |
| wmm video           | Configures video access category wireless multimedia settings       |
| wmm voice           | Configures voice access category wireless multimedia settings       |

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| aifsn <1-15>         | <p>Configures AIFSN (Arbitrary Inter-Frame Space Number) as the wait time between data frames derived from the AIFSN and slot time</p> <ul style="list-style-type: none"> <li>• background – Sets the current AIFSN for low (background) traffic. The default is 7.</li> <li>• best-effort – Sets the current AIFSN for normal (best-effort) traffic. The default is 3.</li> <li>• video – Set the current AIFSN for video traffic. Higher-priority traffic video categories should have lower AIFSNs than lower-priority traffic categories. This causes lower-priority traffic to wait longer before attempting access. The default is 1.</li> <li>• voice – Sets the current AIFSN for voice traffic. Higher-priority traffic voice categories should have lower AIFSNs than lower-priority traffic categories. This causes lower-priority traffic to wait longer before attempting access. The default is 1.</li> </ul> <p>The following keyword is common to all of the above traffic types:</p> <ul style="list-style-type: none"> <li>• &lt;1-15&gt; – Sets a value from 1 - 15</li> </ul> |
| cw-max <0-15>        | <p>Clients pick a number between 0 and the min contention window to wait before retransmission. Clients then double their wait time on a collision, until it reaches the maximum contention window.</p> <ul style="list-style-type: none"> <li>• background – Sets CW Max for low (background) traffic. The default is 10.</li> <li>• best-effort – Sets CW Max for normal (best effort) traffic. The default is 6.</li> <li>• voice – Sets CW Max for voice traffic. The default is 3.</li> <li>• video – Sets CW Max for video traffic. The default is 4</li> </ul> <p>The following keyword is common to all of the above traffic types:</p> <ul style="list-style-type: none"> <li>• &lt;0-15&gt; – ECW: the contention window. The actual value used is <math>(2^{ECW} - 1)</math>.</li> </ul> <p>Lower values are used for higher priority traffic (like video and voice) and higher values are used for lower priority traffic (like background and best-effort).</p>                                                                                                                      |
| cw-min <0-15>        | <p>Clients select a number between 0 and the min contention window to wait before retransmission. Clients then double their wait time on a collision, until it reaches the maximum contention window.</p> <ul style="list-style-type: none"> <li>• background – Sets CW Min for low (background) traffic. The default is 4.</li> <li>• best-effort – Sets CW Min for normal (best effort) traffic. The default is 4.</li> <li>• voice – Sets CW Min for voice traffic. The default is 2.</li> <li>• video – Sets CW Min for video traffic. The default is 3.</li> </ul> <p>The following keyword is common to all of the above traffic types:</p> <ul style="list-style-type: none"> <li>• &lt;0-15&gt; – ECW: the contention window. The actual value used is <math>(2^{ECW} - 1)</math>.</li> </ul> <p>Lower values are used for higher priority traffic (like video and voice) and higher values are used for lower priority traffic (like background and best-effort).</p>                                                                                                                    |
| txop-limit <0-65535> | <p>Set the interval, in microseconds, during which a particular client has the right to initiate transmissions</p> <ul style="list-style-type: none"> <li>• background – Sets TXOP for low (background) traffic. The default is 0.</li> <li>• best-effort – Sets TXOP for normal (best effort) traffic. The default is 4.</li> <li>• voice – Sets TXOP for voice traffic. The default is 47.</li> <li>• video – Sets TXOP for video traffic. The default is 94.</li> </ul> <p>The following keyword is common to all of the above traffic types:</p> <ul style="list-style-type: none"> <li>• &lt;0-65535&gt; – Specify a value from 0 - 65535 to configure the transmit opportunity limit in 32 microsecond units.</li> </ul> <p>Lower values are used for higher priority traffic (like video and voice) and higher values are used for lower priority traffic (like background and best-effort).</p>                                                                                                                                                                                           |

## Usage Guidelines

Before defining a radio QoS policy, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- To support QoS, each multimedia application, wireless client, and WLAN is required to support WMM.
- WMM enabled clients can co-exist with non-WMM clients on the same WLAN. Non-WMM clients are always assigned a Best Effort access category.
- Default WMM values are recommended for all deployments. Changing these values can lead to unexpected traffic blockages, and the blockages might be difficult to diagnose.
- Overloading an access point radio with too much high priority traffic (especially voice) degrades overall service quality for all users.
- TSPEC admission control is only available with newer voice over WLAN phones. Many legacy voice devices do not support TPSEC or even support WMM traffic prioritization.

## Examples

```
nx9500-6C8809(config-radio-qos-test)#wmm best-effort aifsn 7
nx9500-6C8809(config-radio-qos-test)#wmm voice txop-limit 1
nx9500-6C8809(config-radio-qos-test)#show context
radio-qos-policy test
 wmm best-effort aifsn 7
 wmm voice txop-limit 1
 admission-control voice max-airtime-percent 9
 admission-control voice reserved-for-roam-percent 8
 accelerated-multicast stream-threshold 15
nx9500-6C8809(config-radio-qos-test)#
```

## Related Commands

|                             |                                                                         |
|-----------------------------|-------------------------------------------------------------------------|
| <code>no</code> on page 538 | Reverts or resets 802.11e/wireless multimedia settings to their default |
|-----------------------------|-------------------------------------------------------------------------|

*no*

Negates a command or resets configured settings to their default. When used in the radio QoS policy mode, the `no` command enables the resetting of accelerated multicast parameters, admission control parameters, and MultiMedia parameters.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
no [accelerated-multicast|admission-control|smart-aggregation|wmm|service]
no accelerated-multicast [client-timeout|max-client-streams|max-streams|
overflow-policy|stream-threshold]
no admission-control [firewall-detected-traffic|implicit-tspec|background|
best-effort|video|voice]
no admission-control [firewall-detected-traffic|implicit-tspec]
no admission-control [background|best-effort|video|voice] {max-airtime-percent /
max-clients/max-roamed-clients/reserved-for-roam-percent}
no smart-aggregation {delay|max-mesh-hops|min-aggregation-limit}
no smart-aggregation {delay [background|best-effort|streaming-video|
video-conferencing|voice]/max-mesh-hops|min-aggregation-limit}
no wmm [background|best-effort|video|voice] [aifsn|cw-max|cw-min|txop-limit]
no service admission-control across-reassoc
```

## Parameters

```
no <PARAMETERS>
```

no <PARAMETERS> Negates a command or resets configured settings to their default. When used in the radio QoS policy mode, the no command enables the resetting of accelerated multicast parameters, admission control parameters, and MultiMedia parameters.

## Examples

The following example shows the Radio-qos-policy 'test' settings before the 'no' commands are executed:

```
nx9500-6C8809(config-radio-qos-test)#show context
radio-qos-policy test
 admission-control voice max-airtime-percent 9
 admission-control voice reserved-for-roam-percent 8
 admission-control best-effort max-clients 200
 accelerated-multicast stream-threshold 15
 accelerated-multicast client-timeout 500
nx9500-6C8809(config-radio-qos-test)#
nx9500-6C8809(config-radio-qos-test)#no admission-control best-effort max-clients
nx9500-6C8809(config-radio-qos-test)#no accelerated-multicast client-timeout
```

The following example shows the Radio-qos-policy 'test' settings after the 'no' commands are executed:

```
nx9500-6C8809(config-radio-qos-test)#show context
radio-qos-policy test
 admission-control voice max-airtime-percent 9
 admission-control voice reserved-for-roam-percent 8
 accelerated-multicast stream-threshold 15
nx9500-6C8809(config-radio-qos-test)#
rfs4000-229D58(config-radio-qos-test)#show context
radio-qos-policy test
 service admission-control across-reassoc
rfs4000-229D58(config-radio-qos-test)#
rfs4000-229D58(config-radio-qos-test)#no service admission-control across-reassoc
rfs4000-229D58(config-radio-qos-test)#show context
radio-qos-policy test
rfs4000-229D58(config-radio-qos-test)#
```

# ROLE POLICY

## ROLE-POLICY

---

This chapter summarizes the role policy commands in the CLI command structure.

A well defined role policy simplifies user management, and is a significant aspect of WLAN management. It acts as a role based firewall (much like ACLs) consisting of user-defined roles. Each role has a set of match criteria (filters) used to filter wireless clients. The action taken when a client matches the defined filters, is determined by the IP or MAC ACL associated with the user-defined role. Based on the conditions specified in the IP and/or MAC ACL, clients are granted or denied access to the controller managed network. The role policy also defines the VLAN and data rates assigned to clients provided network access.

A role policy also enables LDAP service, allowing controllers and access points to retrieve user information from the LDAP server. This information is matched with the user-defined role filters to determine if a client matches the role or not, and should be allowed or denied access to the controller managed network.

Use the (config-role-policy) instance to configure role policy related configuration commands. To navigate to the config-role instance, use the following commands:

```
<DEVICE>(config)#role-policy <POLICY-NAME>
nx9500-6C8809(config)#role-policy test
nx9500-6C8809(config-role-policy-test)#?
Role Policy Mode commands:
 default-role Configuration for Wireless Clients not matching any role
 ldap-deadperiod Ldap dead period interval
 ldap-query Set the ldap query mode
 ldap-server Add a ldap server
 ldap-timeout Ldap query timeout interval
 no Negate a command or set its defaults
 user-role Create a role

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-role-policy-test)#
```

### role-policy-commands

The following table summarizes role policy configuration commands:

**Table 49: Role-Policy Config Mode Commands**

| Command                                   | Description                                                                                |
|-------------------------------------------|--------------------------------------------------------------------------------------------|
| <code>default-role</code> on page 1595    | When a client fails to find a matching role, the default action is assigned to that client |
| <code>ldap-deadperiod</code> on page 1596 | Configures the LDAP (Lightweight Directory Access Protocol) dead period interval           |
| <code>ldap-query</code> on page 1597      | Enables LDAP service and specifies the LDAP server query mode                              |
| <code>ldap-server</code> on page 1598     | Configures the LDAP server settings                                                        |
| <code>ldap-timeout</code> on page 1599    | Configures the LDAP query timeout                                                          |
| <code>user-role</code> on page 1600       | Creates a role and associates it to the newly created role policy                          |
| <code>no</code> on page 1627              | Negates a command or reverts settings to their default                                     |



**Note**

For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see **COMMON COMMANDS** on page 640.



**Note**

The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (\_) character. In other words, the name of a device cannot contain an underscore.

*default-role*

Assigns a default role to a wireless client that fails to match any of the user-defined roles

When a wireless client accesses a network, the client's details, retrieved from the LDAP server, are matched against all user-defined roles within the role policy. If the client fails to match any of these user-defined role filters, the client is assigned the default role. The action taken (permit or deny access) is determined by the IP and/or MAC ACL associated with the default role.

**Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

**Syntax**

```
default-role use [ip-access-list|ipv6-access-list|mac-access-list]
default-role use [ip-access-list|ipv6-access-list|mac-access-list] [in|out]
<IP/IPv6/MAC-ACCESS-LIST-NAME> precedence <1-100>
```

## Parameters

```
default-role use [ip-access-list|ipv6-access-list|mac-access-list] [in|out]
<IP/IPv6/MAC-ACCESS-LIST-NAME> precedence <1-100>
```

|                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| default-role use                                                                             | Enables default role configuration. This role is applied to a wireless client not matching any of the user-defined roles. <ul style="list-style-type: none"><li>Use – Associates an IP, IPv6, or MAC access list with the default role</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| [ip-access-list ipv6-access-list mac-access-list] [in out]<br><IP/IPv6/MAC-ACCESS-LIST-NAME> | Associates an IP access list, IPv6 access list, or a MAC access list with this default role <ul style="list-style-type: none"><li>in – Applies the rule (IP, IPv6, or MAC) to incoming packets</li><li>out – Applies the rule (IP, IPv6, or MAC) to outgoing packets</li></ul> <p>IP and MAC ACLs act as firewalls by blocking and/or permitting data traffic in both directions (inbound and outbound) within a managed network. IP ACLs use IP addresses for matching operations. Whereas, MAC ACLs use MAC addresses for matching operations. In case of a match (i.e. if a packet is received from or is destined for a specified IP or MAC address), an action is taken. This action is a typical allow, deny or mark designation to controller packet traffic. For more information on ACLs, see <a href="#">ACCESS-LIST</a> on page 1360.</p> <ul style="list-style-type: none"><li>&lt;IP/IPv6/MAC-ACCESS-LIST-NAME&gt; – Specify the access list name.</li></ul> <p>The ACL applied determines the action applied to a client assigned the default role.</p> |
| precedence <1-100>                                                                           | The following keyword is common to the all of the above parameters: <ul style="list-style-type: none"><li>precedence – Assigns a precedence value to the ACL identified in the previous step.<ul style="list-style-type: none"><li>&lt;1-100&gt; – Specify a precedence from 1 - 100.</li></ul></li></ul> <p>ACLs are applied in increasing order of their precedence. Rules with lower precedence are given priority.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## Examples

```
nx9500-6C8809(config-role-policy-test)#default-role use ip-access-list in test precedence 1
nx9500-6C8809(config-role-policy-test)#show context
role-policy test
 default-role use ip-access-list in test precedence 1
nx9500-6C8809(config-role-policy-test)#
```

## Related Commands

|                                 |                                                  |
|---------------------------------|--------------------------------------------------|
| <a href="#">no</a> on page 1627 | Removes or resets the default role configuration |
|---------------------------------|--------------------------------------------------|

### *ldap-deadperiod*

Configures LDAP dead period interval

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000



## Syntax

ldap-deadperiod <60-300>

## Parameters

ldap-deadperiod <60-300>

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ldap-deadperiod <60-300> | <p>Configures an LDAP dead period. When enabled, LDAP service allows the AP or controller to bind with the LDAP server and retrieve user details to match with user-defined role filters. The LDAP deadperiod is the interval between two consecutive attempts to bind with the LDAP server. To enable LDAP service, use the <a href="#">ldap-query</a> on page 1597 command.</p> <ul style="list-style-type: none"><li>• &lt;60-300&gt; – Specify the interval from 60 - 600 seconds. The default is 120 seconds.</li></ul> |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-role-policy-test)#ldap-deadperiod 100
nx9500-6C8809(config-role-policy-test)#show context
role-policy test
 default-role use ip-access-list in test precedence 1
 ldap-deadperiod 100
nx9500-6C8809(config-role-policy-test)#
```

## Related Commands

|                                 |                                                |
|---------------------------------|------------------------------------------------|
| <a href="#">no</a> on page 1627 | Removes or resets the LDAP deadperiod interval |
|---------------------------------|------------------------------------------------|

## ldap-query

Enables LDAP service and specifies the LDAP server query mode

Configuring the LDAP server query mode automatically enables LDAP service on this role policy. By default LDAP service is disabled.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

ldap-query [self|through-controller]

## Parameters

ldap-query [self|through-controller]

|                    |                                                                                                                                                                                                                                   |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| self               | Configures LDAP query mode as <b>self</b> . The AP directly queries the LDAP server for user information. Select 'self' to use local LDAP server resources configured using the <a href="#">ldap-server</a> on page 1598 command. |
| through-controller | Configures LDAP query mode as <b>through-controller</b> . The AP queries the LDAP server, for user information, through the controller. Use this option when the AP is layer 2 adopted to the controller.                         |

## Examples

```
nx9500-6C8809(config-role-policy-test)#ldap-query self
nx9500-6C8809(config-role-policy-test)#show context
role-policy test
 default-role use ip-access-list in test precedence 1
 ldap-query self
 ldap-deadperiod 100
nx9500-6C8809(config-role-policy-test)#
```

## Related Commands

|                                 |                                           |
|---------------------------------|-------------------------------------------|
| <a href="#">no</a> on page 1627 | Disables LDAP service on this role policy |
|---------------------------------|-------------------------------------------|

### *ldap-server*

Associates a specified LDAP server with this role policy. Use this command to configure the credentials needed to bind with the LDAP server.

When enabled, LDAP service allows the AP or controller to bind with the LDAP server and retrieve user details. This information is matched with the user-defined roles within the role policy. If a match is made, the user is assigned the role and allowed or denied access to the controller managed network.

You can associate two LDAP servers with a role policy, allowing failover in case the primary server is unreachable.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
ldap-server <1-2> host [<IP>|<FQDN>] bind-dn <BIND-DN> base-dn <BASE-DN>
bind-password <PASSWORD> {port <1-65535>} {(server-type [active-directory/openldap])}
```

### Parameters

```
ldap-server <1-2> host [<IP>|<FQDN>] bind-dn <BIND-DN> base-dn <BASE-DN>
bind-password <PASSWORD> {port <1-65535>} {(server-type [active-directory/openldap])}
```

|                          |                                                                                                                                                       |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| ldap-server <1-2>        | Specify the LDAP server ID from 1 - 2.<br>The primary LDAP server (ID 1) is used to bind and query. The secondary LDAP server (ID 2) is for failover. |
| host [<IP> <FQDN>]       | Specify the LDAP server's IP address or FQDN (Fully Qualified Domain Name).                                                                           |
| bind-dn <BIND-DN>        | Specify the bind distinguished name (used for binding with the server).                                                                               |
| base-dn <BASE-DN>        | Specify the base distinguished name (used for searching). This should not exceed 127 characters.                                                      |
| bind-password <PASSWORD> | Specify the LDAP server password associated with the bind DN.                                                                                         |

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| port <1-65535>                           | Optional. Specify the LDAP server port from 1 - 65535. (default is 389).                                                                                                                                                                                                                                                                                                                        |
| server-type [active-directory  openldap] | The following keywords are common to the 'port' parameter: <ul style="list-style-type: none"> <li>server-type – Optional. Specifies the LDAP server type <ul style="list-style-type: none"> <li>active-directory – Enables support for active directory attribute search. This is the default setting.</li> <li>openldap – Enables support for openLDAP attribute search</li> </ul> </li> </ul> |

### Usage Guidelines

Use the `ldap-query` command to enable LDAP service on a role policy.

Use the `show > role > ldap-stats` command to view LDAP server status and state.

### Examples

```

nx9500-6C8809(config-role-policy-test)#ldap-server 1 host 192.168.13.7 bind-dn
"CN=Administrator,CN=Users,DC=TechPub,DC=com" base-dn "CN=Administrator,CN=Users,
DC=TechPub,DC=com" bind-password 0 superuser port 2
nx9500-6C8809(config-role-policy-test)#
nx9500-6C8809(config-role-policy-test)#show context
role-policy test
 default-role use ip-access-list in test precedence 1
 ldap-query self
 ldap-deadperiod 100
 ldap-server 1 host 192.168.13.7 bind-dn CN=Administrator,CN=Users,DC=TechPub,
DC=com base-dn CN=Administrator,CN=Users,DC=com bind-password 0 superuser port 2
nx9500-6C8809(config-role-policy-test)#

```

### Related Commands

|                              |                                            |
|------------------------------|--------------------------------------------|
| <code>no</code> on page 1627 | Removes or resets the LDAP server settings |
|------------------------------|--------------------------------------------|

### *ldap-timeout*

Configures the LDAP timeout interval. This is the interval after which a LDAP query is timed out.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
ldap-timeout <1-5>
```

### Parameters

```
ldap-timeout <1-5>
```

|                    |                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ldap-timeout <1-5> | Configures the LDAP query timeout interval from 1 - 5 seconds (default is 2 seconds)<br>When enabled, LDAP service allows the AP or controller to bind with the LDAP server and query it for user details. The LDAP query timeout is the interval between a request to and the response from the LDAP server. Once this interval is exceeded, the LDAP bind and query is timed out. |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-role-policy-test)#ldap-timeout 1
nx9500-6C8809(config-role-policy-test)#show context
role-policy test default-role use ip-access-list in test precedence 1
 ldap-query self
 ldap-timeout 1
 ldap-deadperiod 100
 ldap-server 1 host 192.168.13.7 bind-dn CN=Adminstrator,CN=Users,DC=TechPub,
DC=com base-dn CN=Administrator,CN=Users,DC=com bind-password 0 superuser port 2
nx9500-6C8809(config-role-policy-test)#
```

## Related Commands

|                              |                                                                 |
|------------------------------|-----------------------------------------------------------------|
| <code>no</code> on page 1627 | Removes or resets the LDAP query timeout to default (2 seconds) |
|------------------------------|-----------------------------------------------------------------|

### *user-role*

Creates a user-defined role and enters its configuration mode. Each role consists of a set of filters and action. The filters are match criteria used to filter wireless clients. And the action defines the action taken when a client matches the specified filters.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
user-role <ROLE-NAME> precedence <1-10000>
```

## Parameters

```
user-role <ROLE-NAME> precedence <1-10000>
```

|                       |                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| user-role <ROLE-NAME> | Configures the user role name <ul style="list-style-type: none"><li>• &lt;ROLE-NAME&gt; Specify a name for this user role.</li></ul>                                                                                                                                                                                                                                                                   |
| precedence <1-10000>  | Sets the precedence for this role <p><b>Note:</b> Lower the precedence, higher is the role priority. Precedence determines the order in which a role is applied. If a wireless client matches multiple roles, the role with the lower precedence is applied before those with higher precedence. While there is no default precedence for a role, two or more roles can share the same precedence.</p> |

## Examples

```
nx9500-6C8809(config-role-policy-test)#user-role testing precedence 10
nx9500-6C8809(config-role-policy-test)#show context
role-policy test
 user-role testing precedence 10
 default-role use ip-access-list in test precedence 1
nx9500-6C8809(config-role-policy-test)#
nx9500-6C8809(config-role-policy-test-user-role-testing)#?
Role Mode commands:
 ap-location AP Location configuration
 assign Assign parameters to the role
```

```

authentication-type Type of Authentication
captive-portal Captive-portal based Role Filter
city City configuration
client-identity Client identity
company Company configuration
country Country configuration
department Department configuration
emailid Emailid configuration
employee-type Employee-type configuration
employeeid Employeeid configuration
encryption-type Type of encryption
group Group configuration
memberOf MemberOf configuration
mu-mac MU MAC address configuration
no Negate a command or set its defaults
radius-user Radius-user configuration
ssid SSID configuration
state State configuration
title Title configuration
use Set setting to use
user-defined User-defined configuration

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal
nx9500-6C8809(config-role-policy-test-user-role-testing)#

```

### Related Commands

|                 |                               |
|-----------------|-------------------------------|
| <code>no</code> | Removes an existing user role |
|-----------------|-------------------------------|

### user-role commands

The following table summarizes the user role configuration commands.

**Table 50: User-Role-Mode Commands**

| Commands                         | Description                                                                                                                      |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <code>ap-location</code>         | Configures an AP deployment location based filter                                                                                |
| <code>assign</code>              | Configures upstream/downstream rate limits and VLAN ID assigned to clients matching the filters defined in the user-defined role |
| <code>authentication-type</code> | Configures an authentication type based filter                                                                                   |
| <code>captive-portal</code>      | Configures a captive portal based filter                                                                                         |
| <code>city</code>                | Configures a city name based filter                                                                                              |
| <code>client-identity</code>     | Associates a client-identity (device fingerprinting) based filter                                                                |
| <code>company</code>             | Configures a company name based filter                                                                                           |
| <code>country</code>             | Configures a country name based filter                                                                                           |

**Table 50: User-Role-Mode Commands (continued)**

| Commands        | Description                                                                                                                      |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------|
| department      | Configures a department name based filter                                                                                        |
| emailid         | Configures a e-mail ID based filter                                                                                              |
| employee-type   | Configures a employee type ID based filter                                                                                       |
| employeeid      | Configures a employee ID based filter                                                                                            |
| encryption-type | Configures an encryption type filter                                                                                             |
| group           | Configures a RADIUS group based filter                                                                                           |
| memberOf        | Assigns an <i>Active Directory</i> (AD) group to this user-defined role                                                          |
| mu-mac          | Configures MAC address and mask based filter                                                                                     |
| no              | Removes or resets the filters configured on this user-defined role                                                               |
| ssid            | Configures a SSID based filter                                                                                                   |
| state           | Configures a user role state to match                                                                                            |
| title           | Configures a 'title' string to match                                                                                             |
| use             | Associates a IP and/or MAC ACL with this role. These ACLs specify the action taken when a client matches this user-defined role. |
| user-defined    | Defines a filter based on an attribute defined in the Active Directory or the OpenLDAP server                                    |

#### ap-location

Configures an AP's deployment location based filter for this user-defined role

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
ap-location [any|contains|exact|not-contains]
ap-location any
ap-location [contains|exact|not-contains] <WORD>
```

#### Parameters

```
ap-location any
```

|                 |                                                                                         |
|-----------------|-----------------------------------------------------------------------------------------|
| ap-location any | Specifies the AP location to match (in an RF Domain) or the AP's resident configuration |
| • any           | Defines an AP's location as any                                                         |

```
ap-location [contains|exact|not-contains] <WORD>
```

|                        |                                                                                                                                                                                                                                                                                    |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ap-location            | Specifies the AP location to match (in an RF Domain) or the AP's resident configuration. Select one of the following filter options: <b>contains</b> , <b>exact</b> , or <b>not-contains</b> .                                                                                     |
| contains<br><WORD>     | Applies role if the associating AP's location contains the location string specified in the role. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the location string to match.</li> </ul>                                                                         |
| exact <WORD>           | Applies role if the associating AP's location exactly matches the string specified in the role. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the exact location string to match.</li> </ul>                                                                     |
| not-contains<br><WORD> | Applies role if the associating AP's location does not contain the location string specified in the role. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the location string. The role is applied if the location does not match the specified string.</li> </ul> |

#### Examples

```

nx9500-6C8809nx9500-6C8809(config-role-policy-test-user-role-testing)#ap-location contains
office
nx9500-6C8809(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
 ap-location contains office
nx9500-6C8809(config-role-policy-test-user-role-testing)#

```

#### Related Commands

|           |                                                                        |
|-----------|------------------------------------------------------------------------|
| <b>no</b> | Removes an AP's deployment location string from this user-defined role |
|-----------|------------------------------------------------------------------------|

#### assign

Configures upstream/downstream rate limits and VLAN ID. Clients matching this user-defined role filters are associated with the specified VLAN, and assigned the specified data rates.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```

assign [rate-limit|VLAN]
assign rate-limit [from-client|to-client] <1-65536>
assign vlan <1-4094>

```

#### Parameters

```

assign rate-limit [from-client|to-client] <1-65536>

```

```
assign rate-limit [from-client|to-client] <1-65536>
```

Assigns an upstream and downstream traffic rate limit

- from-client - Assigns a rate limit, in Kbps, for the upstream (from client) traffic
- to-client - Assigns a rate limit, in Kbps, for the downstream (to client) traffic
- <1-65536> - Specify upstream and/or downstream rate limits from 1 - 65536 Kbps.

**Note:** Wireless clients matching this user-defined role are assigned the configured rate limits.

```
assign vlan <1-4094>
```

```
assign vlan <1-4094>
```

Assigns a VLAN (identified by VLAN's ID). Clients matching this user-defined role are associated with the specified VLAN. The VLAN ID represents the shared SSID each user employs to interoperate within the network (once authenticated by the local RADIUS server). This feature is disabled by default.

- <1-4094> - Specify the VLAN ID from 1 - 4094.

**Note:** A wireless client that fails to match any user-defined role is assigned to the default role (configured as a role policy setting) and is mapped to the default VLAN under the WLAN.

## User Guidelines

ACLs can only be used with tunnel or isolated-tunnel modes. They do not work with the local and automatic modes.

In case of bridge VLAN, the default bridging mode is 'auto'. Change the bridging mode to 'tunnel'. This extends the controller's existing VLAN onto the AP and ensures that wireless clients are served IP addresses.

The VLAN configured under the user-defined role need not exist under the WLAN. But, when using tunneled VLAN bridges, configure an additional bridge VLAN. If the VLAN bridging mode is 'local', no additional VLAN configuration is required.

## Examples

```
rfs4000-229D58(config-role-policy-test-user-role-test)#assign rate-limit to-client 200
rfs4000-229D58(config-role-policy-test-user-role-test)#commit
rfs4000-229D58(config-role-policy-test-user-role-test)#show context
 user-role test precedence 1
 assign vlan 1
 assign rate-limit to-client 200
rfs4000-229D58(config-role-policy-test-user-role-test)#
```

The following examples define a role used to forward the IP traffic from all engineers in Test\_Company, Santa Clara, USA onto VLAN 2.



- 1 Create a new role policy with name 'test-policy'..  
`<DEVICE>(config)#role-policy test-policy`
- 2 Specify the LDAP server used for this role policy.  
`<DEVICE>(config-role-policy-test-policy)#ldap-query self`  
`<DEVICE>(config-role-policy-test-policy)#ldap-server 1 host 192.160.1.1 bind-dn`  
`CN=Administrator,CN=Users,DC=testtest,DC=com base-dn CN=Administrator,CN=Users,`  
`DC=com bind-password 0 test port 389`  
`<DEVICE>(config-role-policy-test-policy)#ldap-timeout 2`
- 3 Create a user-defined role.  
`<DEVICE>(config-role-policy-test-policy)#user-role SCEngineer precedence 100`
- 4 Define the role by adding appropriate values and match operators.  
`<DEVICE>(config-role-policy-test-policy-user-role-SCEngineer)#city exact santa-clara`  
`<DEVICE>(config-role-policy-test-policy-user-role-SCEngineer)#company exact`  
`ExampleCompany`  
`<DEVICE>(config-role-policy-test-policy-user-role-SCEngineer)#country exact usa`  
`<DEVICE>(config-role-policy-test-policy-user-role-SCEngineer)#title contains engineer`  
`<DEVICE>(config-role-policy-test-policy-user-role-SCEngineer)#assign vlan-id 2`
- 5 Apply role policy to an access point.  
`ap7161-99BFA8(config-device-ap7161)# use role-policy test-policy`

#### Related Commands

**no** Removes the upstream and/or downstream rate limits applied to this user-defined role. Also removes the VLAN ID.

#### authentication-type

Configures the authentication-type filter for this user-defined role

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
authentication-type [any|eq|neq]
authentication-type any
authentication-type [eq|neq] [eap|kerberos|mac-auth|none]
{ (eap/kerberos/mac-auth/none) }
```

#### Parameters

```
authentication-type any
```

**any** The authentication type is any (eq or neq). This is the default setting.

```
authentication-type [eq|neq] [eap|kerberos|mac-auth|none]
{ (eap/kerberos/mac-auth/none) }
```

|                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>eq [eap kerberos  mac-auth none]</code>  | <p>The role is applied only when the authentication type matches (equals) one or more than one of the following types:</p> <ul style="list-style-type: none"> <li>• eap – Extensible authentication protocol</li> <li>• kerberos – Kerberos authentication</li> <li>• mac-auth – MAC authentication protocol</li> <li>• none – no authentication used</li> </ul> <p><b>Note:</b> These parameters are recursive, and you can configure more than one unique authentication type for this user-defined role.</p>          |
| <code>neq [eap kerberos  mac-auth none]</code> | <p>The role is applied only when the authentication type does not match (not equals) any of the following types:</p> <ul style="list-style-type: none"> <li>• eap – Extensible authentication protocol</li> <li>• kerberos – Kerberos authentication</li> <li>• mac-auth – MAC authentication protocol</li> <li>• none – no authentication used</li> </ul> <p><b>Note:</b> These parameters are recursive, and you can configure more than one unique 'not equal to' authentication type for this user-defined role.</p> |

#### Examples

```

nx9500-6C8809(config-role-policy-test-user-role-testing)#authentication-type eq kerberos
nx9500-6C8809(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
 authentication-type eq kerberos
 ap-location contains office
nx9500-6C8809(config-role-policy-test-user-role-testing)#

```

#### Related Commands

|                 |                                                                              |
|-----------------|------------------------------------------------------------------------------|
| <code>no</code> | Removes the authentication type filter configured for this user-defined role |
|-----------------|------------------------------------------------------------------------------|

#### captive-portal

Configures a captive portal based filter for this user-defined role. A captive portal is a guest access policy that provides temporary and restrictive access to the wireless network. When applied to a WLAN, a captive portal policy ensures secure guest access.

This command defines user-defined role filters based on a wireless client's state of authentication.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
captive-portal authentication-state [any|post-login|pre-login]
```

#### Parameters

```
captive-portal authentication-state [any|post-login|pre-login]
```

|                      |                                                                                                                                                                                                                                           |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| authentication-state | Defines the authentication state of a client connecting to a captive portal                                                                                                                                                               |
| any                  | Specifies any authentication state (authenticated and pending authentication). This is the default setting.<br>This option makes no distinction on whether authentication is conducted before or after the wireless client has logged in. |
| post-login           | Specifies authentication is completed successfully<br>This option requires the wireless client to share authentication credentials after logging into the managed network.                                                                |
| pre-login            | Specifies authentication is pending<br>This option enables captive portal client authentication before the client is logged into the controller.                                                                                          |

### Examples

```

nx9500-6C8809(config-role-policy-test-user-role-testing)#captive-portal authentication-
state pre-login
nx9500-6C8809(config-role-policy-test-user-role-testing)#show context
user-role testing precedence 10
authentication-type eq kerberos
ap-location contains office
captive-portal authentication-state pre-login
nx9500-6C8809(config-role-policy-test-user-role-testing)#

```

### Related Commands

|           |                                                       |
|-----------|-------------------------------------------------------|
| <b>no</b> | Removes the captive portal based role filter settings |
|-----------|-------------------------------------------------------|

### city

Configures a wireless client filter based on the city name

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```

city [any|contains|exact|not-contains]
city [any|exact <WORD>|contains <WORD>|not-contains <WORD>]

```

### Parameters

```

city [any|exact <WORD>|contains <WORD>|not-contains <WORD>]

```

|                 |                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| city            | Specifies a wireless client filter based on how the 'city' name, returned by the RADIUS server, matches the provided expression. Select one of the following options: <b>any</b> , <b>contains</b> , <b>exact</b> , or <b>not-contains</b> .                                                                                                                    |
| any             | No specific city associated with this user-defined role. This role can be applied to any wireless client from any city.                                                                                                                                                                                                                                         |
| contains <WORD> | The role is applied only when the city name, returned by the RADIUS server, contains the string specified in the role. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specify the string to match (this is case sensitive, and is compared against the city name returned by the RADIUS server). It should contain the provided expression.</li> </ul> |

|                        |                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| exact<br><WORD>        | The role is applied only when the city name, returned by the RADIUS server, exactly matches the string specified in the role. <ul style="list-style-type: none"> <li>&lt;WORD&gt; – Specify the exact string to match (this is case sensitive, and is compared against the city name returned by the RADIUS server). It should be an exact match.</li> </ul>                  |
| not-contains<br><WORD> | The role is applied only when the city name, returned by the RADIUS server, does not contain the string specified in the role. <ul style="list-style-type: none"> <li>&lt;WORD&gt; – Specify the string not to match (this is case sensitive, and is compared against the city name returned by the RADIUS server). It should not contain the provided expression.</li> </ul> |

### Examples

```
nx9500-6C8809(config-role-policy-test-user-role-testing)#city exact SanJose
nx9500-6C8809(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
 authentication-type eq kerberos
 ap-location contains office
 captive-portal authentication-state pre-login
 city exact SanJose
nx9500-6C8809(config-role-policy-test-user-role-testing)#
```

### Related Commands

|           |                                                              |
|-----------|--------------------------------------------------------------|
| <b>no</b> | Removes the city name configured with this user-defined role |
|-----------|--------------------------------------------------------------|

### client-identity

Associates a client-identity (device fingerprinting) based filter. The role is assigned to a wireless client matching any of the defined client identities.

For more information on configuring client identity fingerprints, see [client-identity](#).

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
client-identity <CLIENT-IDENTITY-NAME> {<CLIENT-IDENTITY-NAME>}
```

### Parameters

```
client-identity <CLIENT-IDENTITY-NAME> {<CLIENT-IDENTITY-NAME>}
```

|                                        |                                                                                                                                                                                                                                                                                                          |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| client-identity <CLIENT-IDENTITY-NAME> | Specifies the client-identity fingerprint to match (should be existing and configured) <ul style="list-style-type: none"> <li>&lt;CLIENT-IDENTITY-NAME&gt; – Specify the client identity signature name.</li> </ul> <p><b>Note:</b> Multiple client identities can be configured with a role policy.</p> |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### User Guidelines

When associating a single or multiple client identities with a role policy, ensure that a client identity group, containing all the client identities used by the role policy, is attached to the device or profile using the role policy. In other words, group all the client identities (used in this role policy) in a client identity group, and associate this group to the profile or device using this role policy.

For more information on configuring client identities and client identity groups, see [client-identity](#) and [client-identity-group](#)

For more information on associating a client identity group and a role policy to a profile or a device, see [use](#) on page 1232.

#### Examples

```
rfs4000-229D58(config-role-policy-test-user-role-test)#client-identity TestClientIdentity
rfs4000-229D58(config-role-policy-test-user-role-test)#client-identity
ClientIdentityWindows
rfs4000-229D58(config-role-policy-test-user-role-test)#show context
 user-role test precedence 1
 client-identity TestClientIdentity
 client-identity ClientIdentityWindows
rfs4000-229D58(config-role-policy-test-user-role-test)#
```

#### Related Commands

|           |                                                                |
|-----------|----------------------------------------------------------------|
| <b>no</b> | Removes the client identities associated with this role policy |
|-----------|----------------------------------------------------------------|

#### company

Configures a wireless client filter based on the company name

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
company [any|contains|exact|not-contains]
company [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

#### Parameters

```
company [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

|                     |                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| company             | Specifies a wireless client filter based on how the 'company' name, returned by the RADIUS server, matches the provided expression. Select one of the following options: <b>any</b> , <b>contains</b> , <b>exact</b> , or <b>not-contains</b> .                                                                                                                                     |
| any                 | No specific company associated with this user-defined role. This role is applied to any wireless client from any company (no strings to match). This is the default setting.                                                                                                                                                                                                        |
| contains <WORD>     | The role is applied only when the company name, returned by the RADIUS server, contains the string specified in the role. <ul style="list-style-type: none"><li>• &lt;WORD&gt; – Specify the string to match (this is case sensitive, and is compared against the company name returned by the RADIUS server). It should contain the provided expression.</li></ul>                 |
| exact <WORD>        | The role is applied only when the company name, returned by the RADIUS server, exactly matches the string specified in the role. <ul style="list-style-type: none"><li>• &lt;WORD&gt; – Specify the exact string to match (this is case sensitive, and is compared against the company name returned by the RADIUS server). It should be an exact match.</li></ul>                  |
| not-contains <WORD> | The role is applied only when the company name, returned by the RADIUS server, does not contain the string specified in the role. <ul style="list-style-type: none"><li>• &lt;WORD&gt; – Specify the string not to match (this is case sensitive, and is compared against the company name returned by the RADIUS server). It should not contain the provided expression.</li></ul> |

## Examples

```
nx9500-6C8809(config-role-policy-test-user-role-testing)#company exact ExampleCompany
nx9500-6C8809(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
 authentication-type eq kerberos
 ap-location contains office
 captive-portal authentication-state pre-login
 city exact SanJose
 company exact ExampleCompany
nx9500-6C8809(config-role-policy-test-user-role-testing)#
```

## Related Commands

|           |                                                                 |
|-----------|-----------------------------------------------------------------|
| <b>no</b> | Removes the company name configured with this user-defined role |
|-----------|-----------------------------------------------------------------|

## country

Configures a wireless client filter based on the country name

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
country [any|contains|exact|not-contains]
country [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

## Parameters

```
country [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

|                     |                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| country             | Specifies a wireless client filter based on how the 'country' name, returned by the RADIUS server, matches the provided expression. Select one of the following options: <b>any</b> , <b>contains</b> , <b>exact</b> , or <b>not-contains</b> .                                                                                                                                     |
| any                 | No specific country associated with this user-defined role. This role is applied to any wireless client from any country (no strings to match). This is the default setting.                                                                                                                                                                                                        |
| contains <WORD>     | The role is applied only when the country name, returned by the RADIUS server, contains the string specified in the role. <ul style="list-style-type: none"><li>• &lt;WORD&gt; - Specify the string to match (this is case sensitive, and is compared against the country name returned by the RADIUS server). It should contain the provided expression.</li></ul>                 |
| exact <WORD>        | The role is applied only when the country name, returned by the RADIUS server, exactly matches the string specified in the role. <ul style="list-style-type: none"><li>• &lt;WORD&gt; - Specify the exact string to match (this is case sensitive, and is compared against the country name returned by the RADIUS server). It should be an exact match.</li></ul>                  |
| not-contains <WORD> | The role is applied only when the country name, returned by the RADIUS server, does not contain the string specified in the role. <ul style="list-style-type: none"><li>• &lt;WORD&gt; - Specify the string not to match (this is case sensitive, and is compared against the country name returned by the RADIUS server). It should not contain the provided expression.</li></ul> |

## Examples

```
nx9500-6C8809(config-role-policy-test-user-role-testing)#country exact America
nx9500-6C8809(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
```

```

authentication-type eq kerberos
ap-location contains office
captive-portal authentication-state pre-login
city exact SanJose
company exact Examplecompany
country exact America
nx9500-6C8809(config-role-policy-test-user-role-testing)#

```

#### Related Commands

|           |                                                                 |
|-----------|-----------------------------------------------------------------|
| <b>no</b> | Removes the country name configured with this user-defined role |
|-----------|-----------------------------------------------------------------|

#### emailid

Configures a wireless client filter based on the e-mail ID

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```

emailid [any|contains|exact|not-contains]
emailid [any|exact <WORD>|contains <WORD>|not-contains <WORD>]

```

#### Parameters

```

emailid [any|exact <WORD>|contains <WORD>|not-contains <WORD>]

```

|                        |                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| emailid                | Specifies a wireless client filter based on how the 'e-mail ID', returned by the RADIUS server, matches the provided expression. Select one of the following options: <b>any</b> , <b>contains</b> , <b>exact</b> , or <b>not-contains</b> .                                                                                                                                    |
| any                    | No specific e-mail ID associated with this user-defined role. This role can be applied to any wireless client having any e-mail ID (no strings to match). This is the default setting.                                                                                                                                                                                          |
| contains<br><WORD>     | The role is applied only when the e-mail ID, returned by the RADIUS server, contains the string specified in the role. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the string to match (this is case sensitive, and is compared against the e-mail ID returned by the RADIUS server). It should contain the provided expression.</li> </ul>                 |
| exact<br><WORD>        | The role is applied only when the e-mail ID, returned by the RADIUS server, exactly matches the string specified in the role. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the exact string to match (this is case sensitive, and is compared against the e-mail ID returned by the RADIUS server). It should be an exact match.</li> </ul>                  |
| not-contains<br><WORD> | The role is applied only when the e-mail ID, returned by the RADIUS server, does not contain the string specified in the role. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the string not to match (this is case sensitive, and is compared against the e-mail ID returned by the RADIUS server). It should not contain the provided expression.</li> </ul> |

#### Examples

```

nx9500-6C8809(config-role-policy-test-user-role-testing)#emailid exact testing@
examplecompany.com
nx9500-6C8809(config-role-policy-test-user-role-testing)#show context
user-role testing precedence 10
authentication-type eq kerberos
ap-location contains office

```

```

captive-portal authentication-state pre-login
city exact SanJose
company exact ExampleCompany
country exact America
department exact TnV
emailid exact testing@examplecompany.com
nx9500-6C8809(config-role-policy-test-user-role-testing)#

```

### Related Commands

|           |                                                              |
|-----------|--------------------------------------------------------------|
| <b>no</b> | Removes the e-mail ID configured with this user-defined role |
|-----------|--------------------------------------------------------------|

### department

Configures a wireless client filter based on the department name

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```

department [any|contains|exact|not-contains]
department [any|exact <WORD>|contains <WORD>|not-contains <WORD>]

```

### Parameters

```

department [any|exact <WORD>|contains <WORD>|not-contains <WORD>]

```

|                     |                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| department          | Specifies a wireless client filter based on how the 'department' name, returned by the RADIUS server, matches the provided expression. Select one of the following options: <b>any</b> , <b>contains</b> , <b>exact</b> , or <b>not-contains</b> .                                                                                                                                          |
| any                 | No specific department associated with this user-defined role. This role can be applied to any wireless client from any department (no strings to match). This is the default setting.                                                                                                                                                                                                      |
| contains <WORD>     | The role is applied only when the department name, returned by the RADIUS server, contains the string specified in the role. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specify the string to match (this is case sensitive, and is compared against the department name returned by the RADIUS server). It should contain the provided expression.</li> </ul>                 |
| exact <WORD>        | The role is applied only when the department name, returned by the RADIUS server, exactly matches the string specified in the role. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specify the exact string to match (this is case sensitive, and is compared against the department name returned by the RADIUS server). It should be an exact match.</li> </ul>                  |
| not-contains <WORD> | The role is applied only when the department name, returned by the RADIUS server, does not contain the string specified in the role. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specify the string not to match (this is case sensitive, and is compared against the department name returned by the RADIUS server). It should not contain the provided expression.</li> </ul> |

### Examples

```

nx9500-6C8809(config-role-policy-test-user-role-testing)#department exact TnV
nx9500-6C8809(config-role-policy-test-user-role-testing)#show context
user-role testing precedence 10
authentication-type eq kerberos

```





```

ap-location contains office
captive-portal authentication-state pre-login
city exact SanJose
company exact ExampleCompany
country exact America
department exact TnV
nx9500-6C8809(config-role-policy-test-user-role-testing)#

```

#### Related Commands

|           |                                                                    |
|-----------|--------------------------------------------------------------------|
| <b>no</b> | Removes the department name configured with this user-defined role |
|-----------|--------------------------------------------------------------------|

### employee-type

Configures a wireless client filter based on the employee type

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```

employee-type [any|contains|exact|not-contains]
employee-type [any|exact <WORD>|contains <WORD>|not-contains <WORD>]

```

#### Parameters

```

employee-type [any|exact <WORD>|contains <WORD>|not-contains <WORD>]

```

|                        |                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| employee-type          | Specifies a wireless client filter based on how the 'employee type', returned by the RADIUS server, matches the provided expression. Select one of the following options: <b>any</b> , <b>contains</b> , <b>exact</b> , or <b>not-contains</b> .                                                                                                                                        |
| any                    | No specific employee type associated with this user-defined role. This role can be applied to any wireless client having any employee type (no strings to match). This is the default setting.                                                                                                                                                                                          |
| contains<br><WORD>     | The role is applied only when the employee type, returned by the RADIUS server, contains the string specified in the role. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the string to match (this is case sensitive, and is compared against the employee type returned by the RADIUS server). It should contain the provided expression.</li> </ul>                 |
| exact<br><WORD>        | The role is applied only when the employee type, returned by the RADIUS server, exactly matches the string specified in the role. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the exact string to match (this is case sensitive, and is compared against the employee type returned by the RADIUS server). It should be an exact match.</li> </ul>                  |
| not-contains<br><WORD> | The role is applied only when the employee type, returned by the RADIUS server, does not contain the string specified in the role. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the string not to match (this is case sensitive, and is compared against the employee type returned by the RADIUS server). It should not contain the provided expression.</li> </ul> |

#### Examples

```

rfs4000-229D58(config-role-policy-test-user-role-test1)#employee-type exact consultant
rfs4000-229D58(config-role-policy-test-user-role-user1)#show context
user-role user1 precedence 1

```



```
employee-type exact consultant
rfs4000-229D58(config-role-policy-test-user-role-user1)#
```

#### Related Commands

|                                                                                         |
|-----------------------------------------------------------------------------------------|
| <code>no</code> Removes the employee type filter configured with this user-defined role |
|-----------------------------------------------------------------------------------------|

#### employeeid

Configures a wireless client filter based on the employee ID

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
employeeid [any|contains|exact|not-contains]
employeeid [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

#### Parameters

```
employeeid [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

|                     |                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| employeeid          | Specifies a wireless client filter based on how the 'employee ID', returned by the RADIUS server, matches the provided expression. Select one of the following options: <b>any</b> , <b>contains</b> , <b>exact</b> , or <b>not-contains</b> .                                                                                                                                    |
| any                 | No specific employee ID associated with this user-defined role. This role can be applied to any wireless client having any employee ID (no strings to match). This is the default setting.                                                                                                                                                                                        |
| contains <WORD>     | The role is applied only when the employee ID, returned by the RADIUS server, contains the string specified in the role. <ul style="list-style-type: none"><li>• &lt;WORD&gt; – Specify the string to match (this is case sensitive, and is compared against the employee ID returned by the RADIUS server). It should contain the provided expression.</li></ul>                 |
| exact <WORD>        | The role is applied only when the employee ID, returned by the RADIUS server, exactly matches the string specified in the role. <ul style="list-style-type: none"><li>• &lt;WORD&gt; – Specify the exact string to match (this is case sensitive, and is compared against the employee ID returned by the RADIUS server). It should be an exact match.</li></ul>                  |
| not-contains <WORD> | The role is applied only when the employee ID, returned by the RADIUS server, does not contain the string specified in the role. <ul style="list-style-type: none"><li>• &lt;WORD&gt; – Specify the string not to match (this is case sensitive, and is compared against the employee ID returned by the RADIUS server). It should not contain the provided expression.</li></ul> |

#### Examples

```
nx9500-6C8809(config-role-policy-test-user-role-testing)#employeeid contains TnVTest1
nx9500-6C8809(config-role-policy-test-user-role-testing)#show context
user-role testing precedence 10
authentication-type eq kerberos
ap-location contains office
captive-portal authentication-state pre-login
city exact SanJose
company exact ExampleCompany
```

```
country exact America
department exact TnV
emailid exact testing@examplecompany.com
employeeid contains TnVTest1
nx9500-6C8809(config-role-policy-test-user-role-testing)#
```

#### Related Commands

|                                                                          |
|--------------------------------------------------------------------------|
| <b>no</b> Removes the employee ID configured with this user-defined role |
|--------------------------------------------------------------------------|

#### encryption-type

Selects the encryption type for this user-defined role. Encryption ensures privacy between Access Points and wireless clients. There are various modes of encrypting communication on a WLAN, such as CCMP (Counter-model CBC-MAC Protocol), WEP (Wired Equivalent Privacy), keyguard, TKIP (Temporal Key Integrity Protocol), etc.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
encryption-type [any|eq|neq]
encryption-type any
encryption-type [eq|neq] [ccmp|keyguard|none|tkip|wep128|wep64]
(ccmp|keyguard|none|tkip|tkip-ccmp|wep128|wep64)
```

#### Parameters

```
encryption-type any
```

|                                                                                                                              |
|------------------------------------------------------------------------------------------------------------------------------|
| any The encryption type can be any one of the listed options (ccmp keyguard tkip wep128 wep64). This is the default setting. |
|------------------------------------------------------------------------------------------------------------------------------|

```
encryption-type [eq|neq] [ccmp|keyguard|none|tkip|wep128|wep64]
(ccmp|keyguard|none|tkip|tkip-ccmp|wep128|wep64)
```

|                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>eq [ccmp keyguard none wep128 wep64]</code>  | <p>The role is applied only if the encryption type equals to one of the following options:</p> <ul style="list-style-type: none"> <li>• <code>ccmp</code>: Encryption mode is CCMP</li> <li>• <code>keyguard</code>: Encryption mode is keyguard. Keyguard encryption shields the master encryption keys from being discovered</li> <li>• <code>none</code>: No encryption mode specified</li> <li>• <code>tkip</code> - Encryption mode is TKIP</li> <li>• <code>wep128</code>: Encryption mode is WEP128</li> <li>• <code>wep64</code>: Encryption mode is WEP64</li> </ul> <p><b>Note:</b> These parameters are recursive, and you can configure more than one encryption type for this user-defined role.</p>             |
| <code>neq [ccmp keyguard none wep128 wep64]</code> | <p>The role is applied only if encryption type is not equal to any of the following options:</p> <ul style="list-style-type: none"> <li>• <code>ccmp</code>: Encryption mode is not equal to CCMP</li> <li>• <code>keyguard</code>: Encryption mode is not equal to keyguard</li> <li>• <code>none</code>: Encryption mode is not equal to none</li> <li>• <code>tkip</code> - Encryption mode is not equal to TKIP</li> <li>• <code>wep128</code>: Encryption mode is not equal to WEP128</li> <li>• <code>wep64</code>: Encryption mode is not equal to WEP64</li> </ul> <p><b>Note:</b> These parameters are recursive, and you can configure more than one 'not equal to' encryption type for this user-defined role.</p> |

### Examples

```

nx9500-6C8809(config-role-policy-test-user-role-testing)#encryption-type eq wep128
nx9500-6C8809(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
 authentication-type eq kerberos
 encryption-type eq wep128
 ap-location contains office
 captive-portal authentication-state pre-login
 city exact SanJose
 company exact ExampleCompany
 country exact America
 department exact TnV
 emailid exact testing@examplecompany.com
 employeeid contains TnVTest1
nx9500-6C8809(config-role-policy-test-user-role-testing)#

```

### Related Commands

|                 |                                                                   |
|-----------------|-------------------------------------------------------------------|
| <code>no</code> | Removes the encryption type configured for this user-defined role |
|-----------------|-------------------------------------------------------------------|

### group

Configures a wireless client filter based on the RADIUS group name

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
group [any|contains|exact|not-contains]
group [any|contains <WORD>|exact <WORD>|not-contains <WORD>]
```

## Parameters

```
group [any|contains <WORD>|exact <WORD>|not-contains <WORD>]
```

|                        |                                                                                                                                                                                                                                                                                                                                                        |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| group                  | Specifies a wireless client filter based on how the RADIUS group name matches the provided expression. Select one of the following options: <b>any</b> , <b>contains</b> , <b>exact</b> , or <b>not-contains</b> .                                                                                                                                     |
| any                    | This user-defined role can fit into any group (no strings to match). This is the default setting.                                                                                                                                                                                                                                                      |
| contains<br><WORD>     | The role is applied only when the RADIUS group name contains the string specified in the role. <ul style="list-style-type: none"><li>• &lt;WORD&gt; – Specify the string to match (this is case sensitive, and is compared against the group name returned by the RADIUS server). It should contain the provided expression.</li></ul>                 |
| exact<br><WORD>        | The role is applied only when the RADIUS group name exactly matches the string specified in the role. <ul style="list-style-type: none"><li>• &lt;WORD&gt; – Specify the exact string to match (this is case sensitive, and is compared against the group name returned by the RADIUS server). It should be an exact match.</li></ul>                  |
| not-contains<br><WORD> | The role is applied only when the RADIUS group name does not contain the string specified in the role. <ul style="list-style-type: none"><li>• &lt;WORD&gt; – Specify the string not to match (this is case sensitive, and is compared against the group name returned by the RADIUS server). It should not contain the provided expression.</li></ul> |

## Examples

```
nx9500-6C8809(config-role-policy-test-user-role-testing)#group contains testgroup
nx9500-6C8809(config-role-policy-test-user-role-testing)#show context
user-role testing precedence 10
 authentication-type eq kerberos
 encryption-type eq wep128
 ap-location contains office
 group contains testgroup
 captive-portal authentication-state pre-login
 city exact SanJose
 company exact Example_company
 country exact America
 department exact TnV
 emailid exact testing@examplecompany.com
 employeeid contains TnVTest1
nx9500-6C8809(config-role-policy-test-user-role-testing)#
```

## Related Commands

|    |                                                         |
|----|---------------------------------------------------------|
| no | Removes the group configured for this user-defined role |
|----|---------------------------------------------------------|

## memberOf

Applies an AD (Active Directory) group filter to this user-defined role. A wireless client can be a member of more than one group within the AD database. This command applies a AD group based firewall, which applies a role to a wireless client only if it belongs to the specified AD group.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

`memberOf <AD-GROUP-NAME>`

#### Parameters

`memberOf <AD-GROUP-NAME>`

|                                             |                                                                                                                                                                                                                     |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>memberOf &lt;AD-GROUP-NAME&gt;</code> | Applies this user-defined role to a client only if the client belongs to the specified AD group <ul style="list-style-type: none"> <li>• <code>&lt;AD-GROUP-NAME&gt;</code> - Specify the AD group name.</li> </ul> |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
rfs4000-229D58(config-role-policy-test-user-role-test)#memberOf ADTestgroup
rfs4000-229D58(config-role-policy-test-user-role-test)#show context
 user-role test precedence 1
 assign vlan 1
 assign rate-limit to-client 200
 memberOf ADTestgroup
rfs4000-229D58(config-role-policy-test-user-role-test)#
```

#### Related Commands

|                 |                                                         |
|-----------------|---------------------------------------------------------|
| <code>no</code> | Removes the AD group assigned to this user-defined role |
|-----------------|---------------------------------------------------------|

## mu-mac

Configures a MAC address and mask based filter for this role policy

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
mu-mac [<MAC> | any]
mu-mac any
mu-mac <MAC> {mask <MAC>}
```

#### Parameters

`mu-mac any`

|                  |                                                                                             |
|------------------|---------------------------------------------------------------------------------------------|
| <code>any</code> | Applies role to any wireless client (no MAC address to match). This is the default setting. |
|------------------|---------------------------------------------------------------------------------------------|

```
mu-mac <MAC> {mask <MAC>}
```

|                               |                                                                                                                                                                                                                                                                |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;MAC&gt;</code>      | Applies role to the wireless client having specified MAC address <ul style="list-style-type: none"> <li>• <code>&lt;MAC&gt;</code> - Sets the MAC address in the AA-BB-CC-DD-EE-FF format</li> </ul>                                                           |
| <code>mask &lt;MAC&gt;</code> | Optional. After specifying the client's MAC address, specify the mask in the <ul style="list-style-type: none"> <li>• AA-BB-CC-DD-EE-FF format. The role is applied to the wireless client exactly matching the specified MAC address and MAC mask.</li> </ul> |

## Examples

```
nx9500-6C8809(config-role-policy-test-user-role-testing)#mu-mac 11-22-33-44-55-66
nx9500-6C8809(config-role-policy-test-user-role-testing)#show context
user-role testing precedence 10
authentication-type eq kerberos
encryption-type eq wep128
ap-location contains office
mu-mac 11-22-33-44-55-66
group contains testgroup
captive-portal authentication-state pre-login
city exact SanJose
company exact ExampleCompany
country exact America
department exact TnV
emailid exact testing@examplecompany.com
employeeid contains TnVTest1
nx9500-6C8809(config-role-policy-test-user-role-testing)#
```

## Related Commands

|           |                                                             |
|-----------|-------------------------------------------------------------|
| <b>no</b> | Removes the MAC address and mask for this user-defined role |
|-----------|-------------------------------------------------------------|

## radius-user

Configures a wireless client filter based on the RADIUS user name

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
radius-user [any|contains|ends-with|exact|not-contains|starts-with]
```

## Parameters

```
radius-user [any|contains|ends-with|exact|not-contains|starts-with]
```

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| radius-user         | Specifies a wireless client filter based on how the 'radius-user' name, returned by the RADIUS server, matches the provided expression. Select one of the following options: any, contains, exact, or not-contains.                                                                                                                                                                                                                                                                                    |
| any                 | No specific RADIUS user name associated with this user-defined role. This role can be applied to any wireless client (no strings to match). This is the default setting.                                                                                                                                                                                                                                                                                                                               |
| contains<br><WORD>  | The role is applied only when the 'radius-user' name, returned by the RADIUS server, contains the string specified in the role. <ul style="list-style-type: none"><li>• &lt;WORD&gt; - Specify the string to match (this is case sensitive, and is compared against the 'radius-user' name returned by the RADIUS server). It should contain the provided expression.</li></ul> <b>Note:</b> You can use the realm or any sub-string of the user name.                                                 |
| ends-with<br><WORD> | Enables role assignment on the basis of the wireless client's "department" and/or "group" <ul style="list-style-type: none"><li>• &lt;WORD&gt; - Specify the string (could be department/group code). For example: 1005000002. In this the last three digits represent the department/group code. The remaining digits represent user's badge number.</li></ul> <b>Note:</b> The role is applied only when the 'radius-user' name, returned by the RADIUS server, ends with the string specified here. |

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| exact<br><WORD>        | <p>The role is applied only when the 'radius-user' name, returned by the RADIUS server, exactly matches the string specified in the role.</p> <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specify the exact string to match (this is case sensitive, and is compared against the 'radius-user' name returned by the RADIUS server). It should be an exact match.</li> </ul> <p><b>Note:</b> Provide the complete user name along with the realm.</p>                                                       |
| not-contains<br><WORD> | <p>The role is applied only when the 'radius-user' name, returned by the RADIUS server, does not contain the string specified in the role.</p> <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specify the string not to match (this is case sensitive, and is compared against the 'radius-user' name returned by the RADIUS server). It should not contain the provided expression.</li> </ul>                                                                                                               |
| starts-with<br><WORD>  | <p>Enables role assignment on the basis of the wireless client's "department" and/or "group" code</p> <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specify the string (could be department/group code). For example: 0026100573. The first three digits represent the department/group code. The remaining digits represent user's badge number.</li> </ul> <p><b>Note:</b> The role is applied only when the 'radius-user' name, returned by the RADIUS server, starts with the string specified here.</p> |

#### Examples

```

nx9500-6C8809(config-role-policy-test-user-role-testing)#radius-user contains test.com
nx9500-6C8809(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 1
 radius-user contains test.com
 company exact ExampleCompany
 emailid exact testing@examplecompany.com
nx9500-6C8809(config-role-policy-test-user-role-testing)#

```

#### Related Commands

|    |                                                             |
|----|-------------------------------------------------------------|
| no | Removes the MAC address and mask for this user-defined role |
|----|-------------------------------------------------------------|

#### ssid

Configures a SSID based filter

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```

ssid [any|exact|contains|not-contains]
ssid any
ssid [exact|contains|not-contains] <WORD>

```

#### Parameters

```
ssid any
```

|          |                                                                                                                                                                                                                          |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ssid any | <p>Specifies a wireless client filter based on how the SSID is specified in a WLAN.</p> <ul style="list-style-type: none"> <li>• any - The role is applied to any SSID location. This is the default setting.</li> </ul> |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
ssid [exact|contains|not-contains] <WORD>
```



|                        |                                                                                                                                                                                                                                                                                                                         |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ssid                   | Specifies a wireless client filter based on how the SSID is specified in a WLAN. This options are: <b>contains, exact, or not-contains.</b>                                                                                                                                                                             |
| exact<br><WORD>        | The role is applied only when the SSID, returned by the RADIUS server, exactly matches the string specified in the role. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the SSID string to match. The SSID is case sensitive and is compared against the SSID configured for the WLAN.</li> </ul>      |
| contains<br><WORD>     | The role is applied only when the SSID, returned by the RADIUS server, contains the string specified in the role. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the SSID string to match. The SSID is case sensitive and is compared against the SSID configured for the WLAN.</li> </ul>             |
| not-contains<br><WORD> | The role is applied only when the SSID, returned by the RADIUS server, does not contain the string specified in the role. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the SSID string not to match. The SSID is case sensitive and is compared against the SSID configured for the WLAN.</li> </ul> |

### Examples

```

nx9500-6C8809(config-role-policy-test-user-role-testing)#ssid not-contains DevUser
nx9500-6C8809(config-role-policy-test-user-role-testing)#show context
user-role testing precedence 10
 ssid not-contains DevUser
 captive-portal authentication-state pre-login
 city exact SanJose
 company exact ExampleCompany
 country exact America
 department exact TnV
 emailid exact testing@examplecompany.com
nx9500-6C8809(config-role-policy-test-user-role-testing)#]

```

### Related Commands

|    |                                                     |
|----|-----------------------------------------------------|
| no | Removes the SSID configured for a user-defined role |
|----|-----------------------------------------------------|

### state

Configures a user role state to match with this user-defined role

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```

state [any|contains|exact|not-contains]
state [any|contains <WORD>|exact <WORD>|not-contains <WORD>]

```

### Parameters

```

state [any|contains <WORD>|exact <WORD>|not-contains <WORD>]

```

|       |                                                                                                                                                                                             |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| state | Specifies a wireless client filter option based on how the RADIUS state matches the provided expression. Select one of the following options: <b>any, contains, exact, or not-contains.</b> |
| any   | This user role can fit any wireless client irrespective of the state (no strings to match).                                                                                                 |

|                        |                                                                                                                                                                                                                                                                                                                                                |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| contains<br><WORD>     | The user role is applied only when the RADIUS state contains the string specified in the role. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the string to match (this is case sensitive, and is compared against the state returned by the RADIUS server). It should contain the provided expression.</li> </ul>            |
| exact<br><WORD>        | The role is applied only when the RADIUS state exactly matches the string specified in the role. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the exact string to match (this is case sensitive, and is compared against the state returned by the RADIUS server). It should be an exact match.</li> </ul>                  |
| not-contains<br><WORD> | The role is applied only when the RADIUS state does not contain the string specified in the role. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the string not to match (this is case sensitive, and is compared against the state returned by the RADIUS server). It should not contain the provided expression.</li> </ul> |

### Examples

```

nx9500-6C8809(config-role-policy-test-user-role-testing)#state exact active
nx9500-6C8809(config-role-policy-test-user-role-testing)#show context
user-role testing precedence 10
ssid not-contains DevUser
captive-portal authentication-state pre-login
city exact SanJose
company exact ExampleCompany
country exact America
department exact TnV
emailid exact testing@examplecompany.com
state exact active
nx9500-6C8809(config-role-policy-test-user-role-testing)#

```

### Related Commands

|           |                                                               |
|-----------|---------------------------------------------------------------|
| <b>no</b> | Removes the 'state' filter string associated with a user role |
|-----------|---------------------------------------------------------------|

### title

Configures a 'title' string to match

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```

title [any|contains|exact|not-contains]
title [any|contains <WORD>|exact <WORD>|not-contains <WORD>]

```

### Parameters

```

title [any|contains <WORD>|exact <WORD>|not-contains <WORD>]

```

|       |                                                                                                                                                                                                                                               |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| title | Specifies a wireless client filter based on how the title string, returned by the RADIUS server, matches the provided expression. Select one of the following options: <b>any</b> , <b>contains</b> , <b>exact</b> , or <b>not-contains</b> . |
| any   | This user role can fit any wireless client irrespective of the title (no strings to match).                                                                                                                                                   |

|                        |                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| contains<br><WORD>     | The user role is applied only when the title string, returned by the RADIUS server, contains the string specified in the role. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the string to match (this is case sensitive, and is compared against the title returned by the RADIUS server). It should contain the provided expression.</li> </ul>            |
| exact<br><WORD>        | The role is applied only when the title string, returned by the RADIUS server, exactly matches the string specified in the role. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the exact string to match (this is case sensitive, and is compared against the title returned by the RADIUS server). It should be an exact match.</li> </ul>                  |
| not-contains<br><WORD> | The role is applied only when the title string, returned by the RADIUS server, does not contain the string specified in the role. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the string not to match (this is case sensitive, and is compared against the title returned by the RADIUS server). It should not contain the provided expression.</li> </ul> |

### Examples

```
nx9500-6C8809(config-role-policy-test-user-role-testing)#title any
```

### Related Commands

|    |                                                               |
|----|---------------------------------------------------------------|
| no | Removes the 'title' filter string configured with a user role |
|----|---------------------------------------------------------------|

use

Configures an access list based firewall with this user role

A firewall is a mechanism enforcing access control, and is considered a first line of defense in protecting proprietary information within the network. The means by which this is accomplished varies, but in principle, firewalls are mechanisms both *blocking* and *permitting* data traffic based on inbound and outbound IP and MAC rules.

IP based firewall rules are specific to source and destination IP addresses and the unique rules and precedence orders assigned. Both IP and non-IP traffic on the same layer 2 interface can be filtered by applying both an IP ACL and a MAC.

A MAC firewall rule uses source and destination MAC addresses for matching operations, where the result is a typical allow, deny or mark designation to packet traffic.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
use [application-policy|bonjour-gw-discovery-policy|ip-access-list|ipv6-access-list|
mac-access-list|url-filter]
use [application-policy|bonjour-gw-discovery-policy]
use [ip-access-list|ipv6-access-list] [in|out] <IP/ipv6-ACCESS-LIST-NAME>
precedence <1-100>
use mac-access-list [in|out] <MAC-ACCESS-LIST-NAME> precedence <1-100>
use url-filter <URL-FILTER-NAME>
```

## Parameters

```
use [application-policy|bonjour-gw-discovery-policy|ip-access-list|ipv6-access-list|
mac-access-list|url-filter]
```

|                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| application-policy<br><POLICY-NAME>              | Uses an existing Application policy with a user role. When associated, the Application policy enforces application assurance for all users using this role. <ul style="list-style-type: none"><li>• &lt;POLICY-NAME&gt; - Specify the Application policy name (should be existing and configured).</li></ul> <p><b>Note:</b> For more information on Application policy, see <a href="#">application-policy</a> on page 267.</p>                                                          |
| bonjour-gw-<br>discovery-policy<br><POLICY-NAME> | Uses an existing Bonjour GW Discovery policy with a user role. When associated, the Bonjour GW Discovery policy is applied for the Bonjour requests coming from this specific user roles. <ul style="list-style-type: none"><li>• &lt;POLICY-NAME&gt; - Specify the Bonjour GW Discovery policy name (should be existing and configured).</li></ul> <p><b>Note:</b> For more information on Bonjour GW Discovery policy, see <a href="#">bonjour-gw-discovery-policy</a> on page 287.</p> |

```
use [ip-access-list|ipv6-access-list] [in|out] <IP/ipv6-ACCESS-LIST-NAME>
precedence <1-100>
```

|                                  |                                                                                                                                                                                                                                                                  |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip-access-list [in out]          | Uses an IPv4 or IPv6 ACL with this user role <ul style="list-style-type: none"><li>• in - Applies the rule to incoming packets</li><li>• out - Applies the rule to outgoing packets</li></ul>                                                                    |
| <IPv4/IPv6-ACCESS-<br>LIST-NAME> | Specify the IPv4/IPv6 access list name.                                                                                                                                                                                                                          |
| precedence <1-100>               | After specifying the name of the access list, specify the precedence applied to it. Based on the packets received, a lower precedence value is evaluated first. <ul style="list-style-type: none"><li>• &lt;1-100&gt; - Sets a precedence from 1 - 100</li></ul> |

```
use mac-access-list [in|out] <MAC-ACCESS-LIST-NAME> precedence <1-100>
```

|                            |                                                                                                                                                                                                                                                                  |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mac-access-list [in out]   | Uses a MAC access list with this user role <ul style="list-style-type: none"><li>• in - Applies the rule to incoming packets</li><li>• out - Applies the rule to outgoing packets</li></ul>                                                                      |
| <MAC-ACCESS-LIST-<br>NAME> | Specify the MAC access list name.                                                                                                                                                                                                                                |
| precedence <1-100>         | After specifying the name of the access list, specify the precedence applied to it. Based on the packets received, a lower precedence value is evaluated first. <ul style="list-style-type: none"><li>• &lt;1-100&gt; - Sets a precedence from 1 - 100</li></ul> |

```
use url-filter <URL-FILTER-NAME>
```

|                                      |                                                                                                                                                                                                                       |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| use url-filter <URL-FILTER-<br>NAME> | Uses an existing URL filter that acts as a Web content filter firewall rule. <ul style="list-style-type: none"><li>• &lt;POLICY-NAME&gt; - Specify the URL filter name (should be existing and configured).</li></ul> |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-role-policy-test-user-role-testing)#use ip-access-list in
test precedence 9
nx9500-6C8809(config-role-policy-test-user-role-testing)#show context
user-role testing precedence 10
 ssid not-contains DevUser
 captive-portal authentication-state pre-login
 city exact SanJose
 company exact ExampleCompany
 country exact America
 department exact TnV
 emailid exact testing@examplecompany.com
 state exact active
use ip-access-list in test precedence 9
nx9500-6C8809(config-role-policy-test-user-role-testing)#
nx9500-6C8809(config-role-policy-bonjour_test-user-role-bonjour_user1)#use bonjour-gw-
discovery-policy role2
nx9500-6C8809(config-role-policy-bonjour_test-user-role-bonjour_user1)#show context
user-role bonjour_user1 precedence 2
use bonjour-gw-discovery-policy role2
nx9500-6C8809(config-role-policy-bonjour_test-user-role-bonjour_user1)#
nx9500-6C8809(config-role-policy-bonjour_test)#show context
role-policy bonjour_test
user-role bonjour_user precedence 1
 mu-mac A4-D1-D2-BF-3D-19
 use bonjour-gw-discovery-policy role1
user-role bonjour_user1 precedence 2
 mu-mac B0-65-BD-4B-BC-09
use bonjour-gw-discovery-policy role2
.....
nx9500-6C8809(config-role-policy-bonjour_test)#
```

## Related Commands

|                                                                                                      |
|------------------------------------------------------------------------------------------------------|
| <b>no</b> Removes an IP, MAC access list, or a Bonjour GW Discovery policy from use with a user role |
|------------------------------------------------------------------------------------------------------|

## user-defined

Enables you to define a filter based on an attribute defined in the Active Directory or the OpenLDAP server

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
user-defined <ATTR-STRING> [any|contains|exact|not-contains]
user-defined <ATTR-STRING> [any|contains <WORD>|exact <WORD>|not-contains <WORD>]
```

## Parameters

```
user-defined <ATTR-STRING> [any|contains <WORD>|exact <WORD>|not-contains <WORD>]
```

|                            |                                                                                                                                                                                                                                               |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| user-defined <ATTR-STRING> | Specify a filter based on an attribute defined in the AD or OpenLDAP server. <ul style="list-style-type: none"><li>• &lt;ATTR-NAME&gt; – Specify the attribute string.</li></ul> After specifying the attribute name, specify the match type. |
| any                        | No specific string to match. This role can be applied to any wireless client. This is the default setting.                                                                                                                                    |

|                        |                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| contains<br><WORD>     | The role is applied only when the user-defined attribute value, returned by the RADIUS server, contains the string specified in the role. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specify the string to match (this is case sensitive, and is compared against the value returned by the RADIUS server). It should contain the provided expression.</li> </ul>                 |
| exact<br><WORD>        | The role is applied only when the user-defined attribute value, returned by the RADIUS server, exactly matches the string specified in the role. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specify the exact string to match (this is case sensitive, and is compared against the value returned by the RADIUS server). It should be an exact match.</li> </ul>                  |
| not-contains<br><WORD> | The role is applied only when the user-defined attribute value, returned by the RADIUS server, does not contain the string specified in the role. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specify the string not to match (this is case sensitive, and is compared against the value returned by the RADIUS server). It should not contain the provided expression.</li> </ul> |

### Examples

```
rfs4000-229D58(config-role-policy-test-user-role-user1)#user-defined office-location exact EcoSpace
rfs4000-229D58(config-role-policy-test-user-role-user1)#show context
 user-role user1 precedence 1
 employee-type exact consultant
 user-defined office-location exact EcoSpace
rfs4000-229D58(config-role-policy-test-user-role-user1)#
```

### Related Commands

|           |                                                                |
|-----------|----------------------------------------------------------------|
| <b>no</b> | Removes the user-defined filter configured with this user role |
|-----------|----------------------------------------------------------------|

no

Negates a command or resets configured settings to their default. When used in the config role policy user-defined role mode, the no command removes or resets settings, such as AP location, authentication type, encryption type, captive portal, etc.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
no [ap-location|assign|authentication-type|captive-portal|city|client-identity|
company|country|department|emailid|employee-type|employeeid|encryption-type|
group|memberOf|mu-mac|radius-user|ssid|state|title|use|user-defined]
no [ap-location|assign|authentication-type|city|client-identity|company|country|
department|emailid|employee-type|employeeid|encryption-type|group|mu-mac|memberOf|ssid|
radius-user|state|title|user-defined]
no captive-portal authentication-state
no use [application-policy|bonjour-gw-discovery-policy|ip-access-list|
ipv6-access-list|mac-access-list|url-filter]
no use [ip-access-list|ipv6-access-list|mac-access-list] [in|out]
<IP/IPv6/MAC-ACCESS-LIST-NAME> precedence <1-100>
no use [application-policy|bonjour-gw-discovery-policy|url-filter]
```

### Parameters

no <PARAMETERS>

`no <PARAMETERS>` Negates a command or resets configured settings to their default. When used in the config role policy user-defined role mode, the `no` command removes or resets settings, such as AP location, authentication type, encryption type, captive portal, etc.

### Usage Guidelines

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

### Examples

The following example shows the Role Policy 'test' User Role 'testing' configuration before the 'no' commands are executed:

```
nx9500-6C8809(config-role-policy-test-user-role-testing)#show context
user-role testing precedence 10
 authentication-type eq kerberos
 encryption-type eq wep128
 ap-location contains office
 mu-mac 11-22-33-44-55-66
 group contains testgroup
 captive-portal authentication-state pre-login
 city exact SanJose
 company exact ExampleCompany
 country exact America
 department exact TnV
 emailid exact testing@examplecompany.com
 employeeid contains TnVTest1
nx9500-6C8809(config-role-policy-test-user-role-testing)#
nx9500-6C8809(config-role-policy-test-user-role-testing)#no authentication-type
nx9500-6C8809(config-role-policy-test-user-role-testing)#no encryption-type
nx9500-6C8809(config-role-policy-test-user-role-testing)#no group
nx9500-6C8809(config-role-policy-test-user-role-testing)#no mu-mac
nx9500-6C8809(config-role-policy-test-user-role-testing)#no ap-location
nx9500-6C8809(config-role-policy-test-user-role-testing)#no employeeid
```

The following example shows the Role Policy 'test' User Role 'testing' configuration after the 'no' commands are executed:

```
nx9500-6C8809(config-role-policy-test-user-role-testing)#show context
user-role testing precedence 10
 captive-portal authentication-state pre-login
 city exact SanJose
 company exact ExampleCompany
 country exact America
 department exact TnV
 emailid exact testing@examplecompany.com
nx9500-6C8809(config-role-policy-test-user-role-testing)#
```

### `no`

Negates a command or resets settings to their default. When used in the config role policy mode, the `no` command removes or resets the role policy settings.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
no [default-role|ldap-deadperiod|ldap-query|ldap-server <1-2>|ldap-timeout|user-role]
no [ldap-deadperiod|ldap-query|ldap-server <1-2>|ldap-timeout]
no default-role use [ip-access-list|ipv6-access-list|mac-access-list]
no default-role use [ip-access-list|ipv6-access-list|mac-access-list] [in|out]
<IP/IPv6/MAC-ACCESS-LIST-NAME> precedence <1-100>
no user-role <ROLE-NAME>
```

## Parameters

```
no <PARAMETERS>
```

no <PARAMETERS> Negates a command or resets settings to their default. When used in the config role policy mode, the no command removes or resets the role policy settings.

## Examples

The following example shows the role policy 'test' setting before the 'no' commands are executed:

```
nx9500-6C8809(config-role-policy-test)#show context
role-policy test
 default-role use ip-access-list in test precedence 1
 ldap-query self
 ldap-timeout 1
 ldap-deadperiod 100
 ldap-server 1 host 192.168.13.7 bind-dn CN=Administrator,CN=Users,DC=TechPub,DC=com base-
dn
 CN=Administrator,CN=Users,DC=com bind-password 0 superuser port 2

nx9500-6C8809(config-role-policy-test)#
nx9500-6C8809(config-role-policy-test)#no ldap-deadperiod
nx9500-6C8809(config-role-policy-test)#no ldap-timeout
nx9500-6C8809(config-role-policy-test)#no ldap-server 1
```

The following example shows the role policy 'test' setting after the 'no' commands are executed:

```
nx9500-6C8809(config-role-policy-test)#show context
role-policy test
 default-role use ip-access-list in test precedence 1
 ldap-query self
nx9500-6C8809(config-role-policy-test)#
```



# SMART RF POLICY

## SMART-RF-POLICY

---

This chapter summarizes SMART RF (Self Monitoring at Run Time RF) management policy commands in the CLI command structure.

A Smart RF management policy defines operating and recovery parameters that can be assigned to groups of access points. A Smart RF policy is designed to scan the network to identify the best channel and transmit power for each access point radio.

A Smart RF policy reduces deployment costs by scanning the RF environment to determine the best channel and transmit power configuration for each managed radio. Smart RF policies when applied to specific RF Domains, apply site specific deployment configurations and self-healing values to groups of devices within pre-defined physical RF coverage areas.

Smart RF centralizes the decision process and makes intelligent RF configuration decisions using information obtained from the RF environment. Smart RF helps reduce ongoing management and maintenance costs through the periodic re-calibration of the network. Re-calibration can be initiated manually or can be automatically scheduled to ensure the RF configuration is optimized to factor for RF environment changes (such as new sources of interference, or neighboring access points).

Smart RF also provides self-healing functions by monitoring the network in real-time, and provides automatic mitigation from potentially problematic events such as radio interference, coverage holes and radio failures. Smart RF employs self-healing to enable a WLAN to better maintain wireless client performance and site coverage during dynamic RF environment changes, which typically require manual re-configuration to resolve.

Smart RF is supported on any RF Domain manager. In standalone environments, an individual wireless controller manages the calibration and monitoring phases. In clustered environments, a single wireless controller is elected a Smart RF master and the remaining cluster members operate as Smart RF clients. In cluster operation, the Smart RF master co-ordinates the calibration and configuration and during the monitoring phase receives information from the Smart RF clients.

Before defining a Smart RF policy, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- The Smart RF calibration process impacts associated users and should not be run during business or production hours. The calibration process should be performed during scheduled maintenance intervals or non-business hours.
- For Smart RF to provide effective recovery, RF planning must be performed to ensure overlapping coverage exists at the deployment site. Smart RF can only provide recovery when access points are deployed appropriately. Smart RF is not a solution, it's a temporary measure. Administrators need to determine the root cause of RF deterioration and fix it. Smart RF history/events can assist.

Keep in mind that if a Smart RF managed radio is operating in WLAN mode on a channel requiring DFS, it will switch channels if radar is detected.

- If Smart RF is enabled, the radio picks a channel defined in the Smart RF policy.

- If Smart RF is disabled, but a Smart RF policy is mapped, the radio picks channels specified in the Smart RF policy
- If no SMART RF policy is mapped, the radio selects a random channel

If the radio is a dedicated sensor, it stops termination on that channel if a neighboring access point detects radar. The access point attempts to come back to its original channel (statically configured or selected by Smart RF) after the channel evacuation period has expired.

Change this behavior using the `dfs-rehome` on page 1104 command from the controller or service platform CLI. This keeps the radio on the newly selected channel and prevents the radio from coming back to the original channel, even after the channel evacuation period.

### Note



Perform RF planning to ensure overlapping coverage exists at a deployment site, for Smart RF to be a viable network performance tool. Smart RF can only provide recovery when access points are deployed appropriately. Smart RF is not a solution, it is a temporary measure. You need to determine the root cause of RF deterioration and fix it. Smart RF history/events can assist in trouble shooting.

Use the (config) instance to configure Smart RF Policy related configuration commands. To navigate to the Smart RF policy instance, use the following commands:

```
<DEVICE> (config)#smart-rf-policy <POLICY-NAME>
nx9500-6C8809(config)#smart-rf-policy testSmartRF
nx9500-6C8809(config-smart-rf-policy-testSmartRF)#?
Smart RF Mode commands:
 area Specify channel list/ power for an area
 assignable-power Specify the assignable power during power-assignment
 avoidance-time Time to avoid a channel once dfs/adaptivity
 avoidance is necessary
 channel-list Select channel list for smart-rf
 channel-width Select channel width for smart-rf
 coverage-hole-recovery Recover from coverage hole
 enable Enable this smart-rf policy
 group-by Configure grouping parameters
 interference-recovery Recover issues due to excessive noise and
 interference
 neighbor-recovery Recover issues due to faulty neighbor radios
 no Negate a command or set its defaults
 select-shutdown Select redundant 2.4GHz Radios to shutdown
 sensitivity Configure smart-rf sensitivity (Modifies various
 other smart-rf configuration items)
 smart-ocs-monitoring Smart off channel scanning

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-smart-rf-policy-testSmartRF)#
```

## smart-rf-policy commands

The following table summarizes Smart RF policy configuration commands.

**Table 51: Smart-RF-Policy Config Mode Commands**

| Command                                             | Description                                                                                                                                                                                                                |
|-----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">area</a> on page 1631                   | Configures the channel list and power for a specified area                                                                                                                                                                 |
| <a href="#">assignable-power</a> on page 1632       | Specifies the power range during power assignment                                                                                                                                                                          |
| <a href="#">avoidance-time</a> on page 1633         | Allows Smart RF-enabled radios to avoid DFS (Dynamic Frequency Selection) and/or adaptivity regulated channels on detection of interference or radar. This command configures the period for which the channel is avoided. |
| <a href="#">channel-list</a> on page 1635           | Assigns the channel list for the selected frequency                                                                                                                                                                        |
| <a href="#">channel-width</a> on page 1635          | Selects the channel width for Smart RF configuration                                                                                                                                                                       |
| <a href="#">coverage-hole-recovery</a> on page 1637 | Enables recovery from errors                                                                                                                                                                                               |
| <a href="#">enable</a> on page 1638                 | Enables the Smart RF policy                                                                                                                                                                                                |
| <a href="#">group-by</a> on page 1639               | Configures grouping parameters                                                                                                                                                                                             |
| <a href="#">interference-recovery</a> on page 1640  | Enables recovery from excessive noise and interference related issues                                                                                                                                                      |
| <a href="#">interference-recovery</a> on page 1640  | Enables recovery from faulty neighbor radios related issues                                                                                                                                                                |
| <a href="#">select-shutdown</a> on page 1643        | Enables selection and shutting down of 2.4 GHz radios, causing interference, in case the CCI (co-channel interference) value exceeds a specified threshold                                                                 |
| <a href="#">sensitivity</a> on page 1645            | Configures Smart RF sensitivity parameters                                                                                                                                                                                 |
| <a href="#">smart-ocs-monitoring</a> on page 1646   | Applies smart OCS (off-channel scanning) instead of dedicated detectors                                                                                                                                                    |
| <a href="#">no</a> on page 1650                     | Negates a command or reverts settings to their default                                                                                                                                                                     |



### Note

For more information on common commands (clrcsr, commit, help, revert, service, show, write, and exit), see [COMMON COMMANDS](#) on page 640.



### Note

The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore ( `_` ) character. In other words, the name of a device cannot contain an underscore.

### *area*

Configures the channel list and power for a specified area

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000

- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
area <AREA-NAME/STRING-ALIAS> channel-list [2.4GHz|5GHz] <CHANNEL-LIST>
```

### Parameters

```
area <AREA-NAME/STRING-ALIAS> channel-list [2.4GHz|5GHz] <CHANNEL-LIST>
```

|                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| area <AREA-NAME/STRING-ALIAS>             | <p>Specifies the area name</p> <ul style="list-style-type: none"> <li>• &lt;AREA-NAME/STRING-ALIAS&gt; - Specify the area name as clear text. Alternately, use a string-alias to specify the area name. If using a string-alias, ensure that the string-alias is existing and configured.</li> </ul> <p><b>Note:</b> For more information on aliases, see <a href="#">alias</a> on page 237.</p>                                                                                                                     |
| channel-list [2.4GHz 5GHz] <CHANNEL-LIST> | <p>Selects the channels for the specified area in the 2.4 GHz or 5.0 GHz band</p> <ul style="list-style-type: none"> <li>• 2.4GHz - Selects the channels for the specified area in the 2.4 GHz band</li> <li>• 5GHz - Selects the channels for the specified area in the 5.0 GHz band</li> </ul> <p>The following keyword is common to the 2.4 GHz and 5.0 GHz bands:</p> <ul style="list-style-type: none"> <li>• &lt;CHANNEL-LIST&gt; - Enter a comma-separated list of channels for the selected band.</li> </ul> |

### Examples

```
rfs4000-229D58(config-smart-rf-policy-test)#area test channel-list 2.4GHz 1,2,3
rfs4000-229D58(config-smart-rf-policy-test)#show context
smart-rf-policy test
 area test channel-list 2.4GHz 1,2,3
rfs4000-229D58(config-smart-rf-policy-test)#
nx9500-6C8809(config)#alias string $AREA Ecospace
nx9500-6C8809(config)#commit
nx9500-6C8809(config-smart-rf-policy-test)#exit
nx9500-6C8809(config-smart-rf-policy-Ecospace)#area $AREA channel-list 5GHz 36,44
nx9500-6C8809(config-smart-rf-policy-Ecospace)#show context
smart-rf-policy Ecospace
 area $AREA channel-list 5GHz 36,44
nx9500-6C8809(config-smart-rf-policy-Ecospace)#
```

### Related Commands

|                                 |                                                      |
|---------------------------------|------------------------------------------------------|
| <a href="#">no</a> on page 1650 | Removes channel list/power configuration for an area |
|---------------------------------|------------------------------------------------------|

### *assignable-power*

Configures the Smart RF power settings over both 2.4 GHz and 5.0 GHz radios

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
assignable-power [2.4GHz|5GHz] [max|min] <1-20>
```

## Parameters

`assignable-power [2.4GHz|5GHz] [max|min] <1-20>`

|                         |                                                                                                                                                                                                                                                                  |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2.4GHz [max min] <1-20> | Assigns a power range on the 2.4 GHz band <ul style="list-style-type: none"><li>max &lt;1-20&gt; - Sets the upper limit from 1 dBm - 20 dBm (default is 17 dBm)</li><li>min &lt;1-20&gt; - Sets the lower limit from 1 dBm - 20 dBm (default is 4 dBm)</li></ul> |
| 5GHz [max min] <1-20>   | Assigns a power range on the 5.0 GHz band <ul style="list-style-type: none"><li>max &lt;1-20&gt; - Sets the upper limit from 1 dBm - 20 dBm (default is 17 dBm)</li><li>min &lt;1-20&gt; - Sets the lower limit from 1 dBm - 20 dBm (default is 4 dBm)</li></ul> |

## Examples

```
nx9500-6C8809(config-smart-rf-policy-test)#assignable-power 2.4GHz max 20
nx9500-6C8809(config-smart-rf-policy-test)#assignable-power 2.4GHz min 8
nx9500-6C8809(config-smart-rf-policy-test)#show context
smart-rf-policy test
 assignable-power 2.4GHz max 20
 assignable-power 2.4GHz min 8
 area test channel-list 2.4GHz 1,2,3
nx9500-6C8809(config-smart-rf-policy-test)#
```

## Related Commands

|                              |                                        |
|------------------------------|----------------------------------------|
| <code>no</code> on page 1650 | Resets assignable power to its default |
|------------------------------|----------------------------------------|

### *avoidance-time*

Allows Smart-RF enabled radios to avoid channels with high levels of interference and channels where radar has been detected

This command configures the interval for which a channel is avoided on detection of interference or radar, and is applicable only if the channel selection mode is set to Smart and a Smart-RF policy is applied to the access point's RF Domain. For more information on configuring a radio's channel of operation, see [channel](#) on page 1098.

Certain 5.0 GHz channels are subject to FCC / ETSI DFS regulations that require channels transmitting critical radar signals to be free of interference from radio signals. Consequently, DFS-enabled 5.0 GHz radios scan and switch channels if radar is detected on their current channel of operation. If radar-free channels are not available, the radio stops transmitting until it identifies a radar-free channel.

Adaptivity is a new EU (European Union) stipulation that requires access points to monitor interference levels on their current channel of operation, and stop functioning on channels with interference levels exceeding ETSI-specified threshold values. When enabled, this feature ensures recovery by switching the radio to a new channel with less interference.

Once adaptivity or DFS is triggered, the radio's channel is switched based on the channel selection mode specified. If the channel is fixed, the radio attempts to come back to its specified channel of operation after the DFS/adaptivity channel evacuation period has expired.



#### Note

To optionally disable the radio from switching back to its original channel of operation, execute the **no > dfs-rehome** command in the radio interface configuration mode of the access point's profile or device. For more information, see [dfs-rehome](#) on page 1104.



#### Note

For radio's with channel selection mode set to **ACS**, **Random**, or **Fixed** adaptivity timeout can be configured in the access point's radio interface mode. For more information, see [adaptivity](#) on page 1076.

On the other hand, if the radio's channel selection mode is set to Smart or ACS, once adaptivity or DFS is triggered, the channel is avoided until the avoidance-time, specified here, expires. Once the evacuation period has expired, the channel is free for use by both Smart-RF and ACS.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
avoidance-time [adaptivity|dfs] <30-3600>
```

#### Parameters

```
avoidance-time [adaptivity|dfs] <30-3600>
```

|                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| avoidance-time [adaptivity dfs] <30-3600> | <p>Configures the time for which a channel is avoided after dfs or adaptivity is triggered</p> <ul style="list-style-type: none"><li>• <b>adaptivity</b> - Sets the time, in minutes, for which a radio avoids an adaptivity-regulated channel detected with interference</li><li>• <b>dfs</b> - Sets the time, in minutes, for which a radio avoids a DFS-regulated channel detected on radar</li><li>• <b>&lt;30-3600&gt;</b> - Specify a value from 30 - 3600 minutes. The default for both parameters is 90 minutes.</li></ul> |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config-smart-rf-policy-test)#avoidance-time adaptivity 200
nx9500-6C8809(config-smart-rf-policy-test)#avoidance-time dfs 300
nx9500-6C8809(config-smart-rf-policy-test)#show context
smart-rf-policy test
assignable-power 2.4GHz max 20
assignable-power 2.4GHz min 8
area test channel-list 2.4GHz 1,2,3
avoidance-time dfs 300
```

```

avoidance-time adaptivity 200
nx9500-6C8809(config-smart-rf-policy-test)#
nx9500-6C8809(config-smart-rf-policy-test)#no avoidance-time adaptivity
nx9500-6C8809(config-smart-rf-policy-test)#show context include-factory | include
avoidance-time
 avoidance-time dfs 300
avoidance-time adaptivity 90
nx9500-6C8809(config-smart-rf-policy-test)#

```

### Related Commands

|                              |                                                                                     |
|------------------------------|-------------------------------------------------------------------------------------|
| <code>no</code> on page 1650 | Reverts the DFS/adaptivity regulated channel avoidance time to default (90 minutes) |
|------------------------------|-------------------------------------------------------------------------------------|

### *channel-list*

Assigns a list of channels, for the selected frequency, used in Smart RF scans

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
channel-list [2.4GHz|5GHz] <WORD>
```

#### Parameters

- `channel-list [2.4GHz|5GHz] <WORD>`

|               |                                                                                                                                                           |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2.4GHz <WORD> | Assigns a channel list for the 2.4 GHz band <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specify a comma separated list of channels</li> </ul> |
| 5GHz <WORD>   | Assigns a channel list for the 5.0 GHz band <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specify a comma separated list of channels</li> </ul> |

#### Examples

```

nx9500-6C8809(config-smart-rf-policy-test)#channel-list 2.4GHz 1,12
nx9500-6C8809(config-smart-rf-policy-test)#show context
smart-rf-policy test
 assignable-power 2.4GHz max 20
 assignable-power 2.4GHz min 8
 channel-list 2.4GHz 1,12
 area test channel-list 2.4GHz 1,2,3
 avoidance-time dfs 300
nx9500-6C8809(config-smart-rf-policy-test)#

```

### Related Commands

|                              |                                                     |
|------------------------------|-----------------------------------------------------|
| <code>no</code> on page 1650 | Removes the channel list for the selected frequency |
|------------------------------|-----------------------------------------------------|

### *channel-width*

Selects the channel width for Smart RF configuration

## Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
channel-width [2.4GHz|5GHz]
channel-width 2.4GHz [20MHz|40MHz|auto]
channel-width 5GHz [20MHz|40MHz|80MHz|auto]
```

## Parameters

```
channel-width 2.4GHz [20MHz|40MHz|auto]
```

|                           |                                                                                                                                                                                                                                                                                                                                                |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2.4GHz [20MHz 40MHz auto] | Assigns the channel width for the 2.4 GHz band <ul style="list-style-type: none"><li>• 20MHz - Assigns the 20 MHz channel width. This is the default setting.</li><li>• 40MHz - Assigns the 40 MHz channel width</li><li>• auto - Auto-selects the channel. Assigns the best possible channel in the 20 MHz or 40 MHz channel width.</li></ul> |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
channel-width 5GHz [20MHz|40MHz|auto]
```

|                                       |                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| channel-width 5GHz [20MHz 40MHz auto] | Assigns the channel width for the 5.0 GHz band <ul style="list-style-type: none"><li>• 20MHz - Assigns the 20 MHz channel width.</li><li>• 40MHz - Assigns the 40 MHz channel width. This is the default setting.</li><li>• 80MHz - Assigns the 80 MHz channel width</li><li>• auto - Auto-selects the channel. Assigns the best possible channel in the 20 MHz or 40 MHz or 80 MHz channel width.</li></ul> |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Usage Guidelines

The 20/40 MHz operation allows the access point to receive packets from clients using 20 MHz, and transmit using 40 MHz. This mode is supported for 802.11n users on both the 2.4 GHz and 5.0 GHz radios. If an 802.11n user selects two channels (a primary and secondary channel), the system is configured for dynamic 20/40 operation. When 20/40 is selected, clients can take advantage of wider channels. 802.11n clients experience improved throughput using 40 MHz while legacy clients (either 802.11a or 802.11b/g depending on the radio selected) can still be serviced without interruption using 20 MHz. Select auto to enable automatic assignment of channels to working radios to avoid channel overlap and avoid interference from external RF sources.

## Examples

```
nx9500-6C8809(config-smart-rf-policy-test)#channel-width 2.4GHz auto
nx9500-6C8809(config-smart-rf-policy-test)#channel-width 5GHz auto
nx9500-6C8809(config-smart-rf-policy-test)#show context
smart-rf-policy test
assignable-power 2.4GHz max 20
assignable-power 2.4GHz min 8
channel-list 2.4GHz 1,12
channel-width 5GHz auto
channel-width 2.4GHz auto
area test channel-list 2.4GHz 1,2,3
```



```
avoidance-time dfs 300
nx9500-6C8809(config-smart-rf-policy-test)#
```

## Related Commands

|                              |                                                                |
|------------------------------|----------------------------------------------------------------|
| <code>no</code> on page 1650 | Resets channel width for the selected frequency to its default |
|------------------------------|----------------------------------------------------------------|

## coverage-hole-recovery

Enables recovery from coverage hole errors detected by Smart RF. Use this command to configure the coverage hole recovery settings.

When coverage hole recovery is enabled, on detection of a coverage hole, Smart RF first determines the power increase needed based on the SNR (signal-to-noise ratio) for a client as seen by the access point radio. If a client's SNR is above the specified threshold, the transmit power is increased until the SNR falls below the threshold.



### Note

The coverage-hole-recovery parameters can be modified only if the sensitivity level is set to 'custom'. For more information, see [sensitivity](#) on page 1645.

## Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
coverage-hole-recovery {client-threshold/coverage-interval/interval/snr-threshold}
coverage-hole-recovery {client-threshold [2.4GHz|5GHz] <1-255>}
coverage-hole-recovery {coverage-interval/interval} [2.4GHz|5GHz] <1-120>
coverage-hole-recovery {snr-threshold [2.4Ghz|5Ghz] <1-75>}
```

## Parameters

```
coverage-hole-recovery {client-threshold [2.4GHz|5GHz] <1-255>}
```

|                  |                                                                                                                                                                            |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| client-threshold | Optional. Specifies the minimum number of clients associated to a radio in order to trigger coverage hole recovery.                                                        |
| 2.4GHz <1-255>   | Specifies the minimum number of clients on the 2.4 GHz band <ul style="list-style-type: none"><li>• &lt;1-255&gt; - Sets a value from 1 - 255. The default is 1.</li></ul> |
| 5GHz <1-255>     | Specifies the minimum number of clients on the 5.0 GHz band <ul style="list-style-type: none"><li>• &lt;1-255&gt; - Sets a value from 1 - 255. The default is 1.</li></ul> |

```
coverage-hole-recovery {coverage-interval/interval} [2.4GHz|5GHz] <1-120>
```

|                   |                                                                                                                        |
|-------------------|------------------------------------------------------------------------------------------------------------------------|
| coverage-interval | Optional. Specifies the interval between the discovery of a coverage hole and the initiation of coverage hole recovery |
| interval          | Optional. Specifies the interval at which coverage hole recovery is performed even before a coverage hole is detected  |

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2.4GHz<br><1-120> | <p>The following keywords are common to the 'coverage-interval' and 'interval' parameters:</p> <ul style="list-style-type: none"> <li>• 2.4GHz &lt;1-120&gt; - Specifies the coverage hole recovery interval on the 2.4 GHz band</li> <li>• &lt;1-120&gt; - Specify a value from 1 - 120 seconds.</li> </ul> <p><b>Note:</b> coverage-interval - The default is 10 seconds.</p> <p><b>Note:</b> interval - The default is 30 seconds.</p> |
| 5GHz <1-120>      | <p>The following keywords are common to the 'coverage-interval' and 'interval' parameters:</p> <ul style="list-style-type: none"> <li>• 5GHz &lt;1-120&gt; - Specifies a coverage hole recovery interval on the 5.0 GHz band</li> <li>• &lt;1-120&gt; - Specify a value from 1 - 120 seconds.</li> </ul> <p><b>Note:</b> coverage-interval - The default is 10 seconds.</p> <p><b>Note:</b> interval - The default is 30 seconds.</p>     |

coverage-hole-recovery {snr-threshold} [2.4Ghz|5Ghz] <1-75>

|               |                                                                                                                                                                                                                                                                |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| snr-threshold | Optional. Specifies the SNR threshold. This value is the SNR threshold for an associated client as seen by its associated AP radio. When the SNR threshold is exceeded, the radio increases its transmit power to increase coverage for the associated client. |
| 2.4GHz <1-75> | <p>Specifies SNR threshold on the 2.4 GHz band</p> <ul style="list-style-type: none"> <li>• &lt;1-75&gt; - Sets a value from 1 dB - 75 dB. The default is 20 dB.</li> </ul>                                                                                    |
| 5GHz <1-75>   | <p>Specifies SNR threshold on the 5.0 GHz band</p> <ul style="list-style-type: none"> <li>• &lt;1-75&gt; - Sets a value from 1 - 75. The default is 20 dB.</li> </ul>                                                                                          |

### Examples

```

nx9500-6C8809(config-smart-rf-policy-test)#coverage-hole-recovery snr-threshold 2.4GHz 35
nx9500-6C8809(config-smart-rf-policy-test)#show context
smart-rf-policy test
sensitivity custom
assignable-power 2.4GHz max 20
assignable-power 2.4GHz min 8
channel-list 2.4GHz 1,12
channel-width 5GHz auto
channel-width 2.4GHz auto
area test channel-list 2.4GHz 1,2,3
avoidance-time dfs 300
coverage-hole-recovery snr-threshold 2.4GHz 35
nx9500-6C8809(config-smart-rf-policy-test)#

```

### Related Commands

|                 |                                             |
|-----------------|---------------------------------------------|
| no on page 1650 | Disables recovery from coverage hole errors |
|-----------------|---------------------------------------------|

### enable

Enables the Smart RF policy

Use this command to enable this Smart RF policy. Once enabled, the policy can be assigned to a RF Domain supporting a network.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

enable

### Parameters

None

### Examples

```
nx9500-6C8809(config-smart-rf-policy-test)#enable
nx9500-6C8809(config-smart-rf-policy-test)#show context include-factory | include
enable
enable
nx9500-6C8809(config-smart-rf-policy-test)#
```

### Related Commands

|                 |                              |
|-----------------|------------------------------|
| no on page 1650 | Disables the Smart RF policy |
|-----------------|------------------------------|

### *group-by*

Enables grouping of APs on the basis of their location in a building (floor) or an area

Within a large RD Domain, grouping of APs (within an area or on the same floor in a building) facilitates statistics gathering and troubleshooting.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

group-by [area|floor]

### Parameters

group-by [area|floor]

|                                                    |                                               |
|----------------------------------------------------|-----------------------------------------------|
| area                                               | Groups radios based on their area of location |
| floor                                              | Groups radios based on their floor location   |
| <b>Note:</b> Both options are disabled by default. |                                               |

## Examples

```
nx9500-6C8809(config-smart-rf-policy-test)#group-by floor
nx9500-6C8809(config-smart-rf-policy-test)#show context
smart-rf-policy test
 group-by floor
 sensitivity custom
 assignable-power 2.4GHz max 20
 assignable-power 2.4GHz min 8
 channel-list 2.4GHz 1,12
 channel-width 5GHz auto
 channel-width 2.4GHz auto
 area test channel-list 2.4GHz 1,2,3
 avoidance-time dfs 300
 coverage-hole-recovery snr-threshold 2.4GHz 35
nx9500-6C8809(config-smart-rf-policy-test)#
```

## Related Commands

|                              |                                 |
|------------------------------|---------------------------------|
| <code>no</code> on page 1650 | Removes Smart RF group settings |
|------------------------------|---------------------------------|

### *interference-recovery*

Enables interference recovery from neighboring radios and other sources of WiFi and non-WiFi interference when excess noise and interference is detected within the Smart RF supported radio coverage area. Smart RF provides mitigation from interference sources by monitoring the noise levels and other RF parameters on an Access Point radio's current channel. When a noise threshold is exceeded, Smart RF can select an alternative channel with less interference. To avoid channel flapping, a hold timer is defined which disables interference avoidance for a specific period of time upon detection. Interference recovery is enabled by default.



#### Note

The `interference-recovery` parameters can be modified only if the sensitivity level is set to 'custom'. For more information, see [sensitivity](#) on page 1645.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
interference-recovery {channel-hold-time|channel-switch-delta|client-threshold|
interference|neighbor-offset|noise|noise-factor}
interference-recovery {channel-switch-delta [2.4GHz|5GHz] <5-35>}
interference-recovery {channel-hold-time <0-86400>|client-threshold <1-255>|
interference|neighbor-offset <3-10>|noise|noise-factor <1.0-3.0>}
```

### Parameters

```
interference-recovery {channel-switch-delta [2.4GHz|5GHz] <5-35>}
```

|                      |                                                                                                                                                                                                                                                                                                                                  |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| channel-switch-delta | Optional. Configures a threshold value for the difference between interference levels on the current channel and the prospective channel needed to trigger a channel change. If the difference in noise levels on the current channel and the prospective channel is below the configured threshold, the channel is not changed. |
| [2.4GHz]<br>5GHz]    | Selects the band <ul style="list-style-type: none"> <li>• 2.4GHz – Selects the 2.4 GHz band</li> <li>• 5GHz – Selects the 5.0 GHz band</li> </ul>                                                                                                                                                                                |
| <5-35>               | Specifies the threshold value for the difference between the current and prospective channel interference levels <ul style="list-style-type: none"> <li>• &lt;5-35&gt; – Sets a value from 5 dBm - 35 dBm. The default setting is 20 dBm for both 2.4 GHz and 5.0 GHz bands.</li> </ul>                                          |

```
interference-recovery {channel-hold-time <0-86400>|client-threshold <1-255>|
interference|neighbor-offset <3-10>|noise|noise-factor <1.0-3.0>}
```

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| channel-hold-time <0-86400> | Optional. Defines the minimum time between two channel change recoveries <ul style="list-style-type: none"> <li>• &lt;0-86400&gt; – Sets the time, in seconds, between channel change assignments based on interference or noise. The default is 1,800 seconds.</li> </ul>                                                                                                                                                                                                                          |
| client-threshold <1-255>    | Optional. Specifies client thresholds needed to avoid channel change. If the specified threshold number of clients are connected to a radio, the radio avoids changing channels even if the Smart RF master determines that a channel change is required. <ul style="list-style-type: none"> <li>• &lt;1-255&gt; – Sets the number of clients from 1 - 255. The default is 50.</li> </ul>                                                                                                           |
| interference                | Optional. Considers external interference values to perform interference recovery. This feature allows the Smart RF policy to scan for excess interference from supported radio devices. WLANs are susceptible to sources of interference, such as neighboring radios, cordless phones, microwave ovens and Bluetooth devices. When interference for WiFi sources is detected, Smart RF supported devices can change the channel and move to a cleaner channel. This feature is enabled by default. |
| neighbor-offset <3-10>      | Optional. Configures a noise factor value, which is taken into consideration when switching channels to avoid interference from neighboring access points. Smart RF enabled access points consider the difference in noise between candidate channels. <ul style="list-style-type: none"> <li>• &lt;3-10&gt; – Specify a noise factor value from 3 - 10.</li> </ul>                                                                                                                                 |
| noise                       | Optional. Considers noise values to perform interference recovery. This feature allows the Smart RF policy to scan for excess noise from WiFi devices. When detected, Smart RF supported devices can change their channel and move to a cleaner channel. This feature is enabled by default.                                                                                                                                                                                                        |
| noise-factor <1.0-3.0>      | Optional. Configures additional noise factor (the level of network interference detected) for non WiFi interference <ul style="list-style-type: none"> <li>• &lt;1.0-3.0&gt; – Specify the noise factor from 1.0 - 3.0. The default is 1.5.</li> </ul>                                                                                                                                                                                                                                              |

## Examples

```
nx9500-6C8809(config-smart-rf-policy-test)#interference-recovery channel-switch-delta
2.4GHz 5
nx9500-6C8809(config-smart-rf-policy-test)#show con
smart-rf-policy test
group-by floor
sensitivity custom
assignable-power 2.4GHz max 20
assignable-power 2.4GHz min 8
channel-list 2.4GHz 1,12
```

```

channel-width 5GHz auto
channel-width 2.4GHz auto
area test channel-list 2.4GHz 1,2,3
avoidance-time dfs 300
interference-recovery channel-switch-delta 2.4GHz 5
coverage-hole-recovery snr-threshold 2.4GHz 35
nx9500-6C8809(config-smart-rf-policy-test)#

```

## Related Commands

|                              |                                                         |
|------------------------------|---------------------------------------------------------|
| <code>no</code> on page 1650 | Disables recovery from excessive noise and interference |
|------------------------------|---------------------------------------------------------|

### *neighbor-recovery*

Enables recovery from errors due to faulty neighboring radios. Enabling neighbor recovery ensures automatic recovery from failed radios within the radio coverage area. Smart RF instructs neighboring access points to increase their transmit power to compensate for the failed radio. Neighbor recovery is enabled by default when the sensitivity setting is medium.



#### Note

The neighbor-recovery parameters can be modified only if the sensitivity level is set to 'custom'. For more information, see [sensitivity](#) on page 1645.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```

neighbor-recovery {dynamic-sampling/power-hold-time/power-threshold}
neighbor-recovery {dynamic-sampling} {retries <1-10>/threshold <1-30>}
neighbor-recovery {power-hold-time <0-3600>}
neighbor-recovery {power-threshold [2.4Ghz|5Ghz] <-85--55>}

```

### Parameters

```
neighbor-recovery {dynamic-sampling} {retries <1-10>/threshold <1-30>}
```

|                  |                                                                                                                                                                                                                                                               |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dynamic-sampling | Optional. Enables dynamic sampling on this Smart RF policy. Dynamic sampling allows you to define how Smart RF adjustments are triggered by locking the 'retry' and 'threshold' values. Dynamic sampling is disabled by default.                              |
| retries <1-10>   | Optional. Specifies the number of retries before allowing a power level adjustments to compensate for a potential coverage hole. <ul style="list-style-type: none"> <li>• &lt;1-10&gt; - Sets the number of retries from 1 - 10. The default is 3.</li> </ul> |
| threshold <1-30> | Optional. Specifies the minimum number of sample reports before which a power change requires dynamic sampling <ul style="list-style-type: none"> <li>• &lt;1-30&gt; - Sets the minimum number of reports from 1 - 30. The default is 5.</li> </ul>           |

```
neighbor-recovery {power-hold-time <0-3600>}
```

|                 |                                                                                                                 |
|-----------------|-----------------------------------------------------------------------------------------------------------------|
| power-hold-time | Optional. Specifies the minimum time, in seconds, between two power changes on a radio during neighbor-recovery |
| <0-3600>        | Sets the time from 0 - 3600 sec. The default is 0 seconds.                                                      |

neighbor-recovery {power-threshold [2.4GHz|5GHz] <-85--55>}

|                 |                                                                                                                                                                                                                                                                                                  |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| power-threshold | Optional. Specifies the power threshold based on which recovery is performed<br>The 2.4 GHz/5.0 GHz radio uses the value specified here as the maximum power increase threshold if the radio is required to increase its output power to compensate for a failed radio within its coverage area. |
| [2.4GHz 5GHz]   | Selects the band <ul style="list-style-type: none"> <li>• 2.4GHz - Selects the 2.4 GHz band</li> <li>• 5GHz - Selects the 5.0 GHz band</li> </ul>                                                                                                                                                |
| <-85--55>       | Specify the threshold value <ul style="list-style-type: none"> <li>• &lt;-85--55&gt; - Sets the power threshold from -85 dBm - -55 dBm. The default is -70 dBm for both the 2.4 GHz and 5.0 GHz bands.</li> </ul>                                                                                |

### Examples

```

nx9500-6C8809(config-smart-rf-policy-test)#neighbor-recovery power-threshold 2.4GHz -82
nx9500-6C8809(config-smart-rf-policy-test)#neighbor-recovery power-threshold 5GHz -65
nx9500-6C8809(config-smart-rf-policy-test)#show context
smart-rf-policy test
 group-by floor
 sensitivity custom
 assignable-power 2.4GHz max 20
 assignable-power 2.4GHz min 8
 channel-list 2.4GHz 1,12
 channel-width 5GHz auto
 channel-width 2.4GHz auto
 area test channel-list 2.4GHz 1,2,3
 avoidance-time dfs 300
 interference-recovery channel-switch-delta 2.4GHz 5
 neighbor-recovery power-threshold 5GHz -65
 neighbor-recovery power-threshold 2.4GHz -82
 coverage-hole-recovery snr-threshold 2.4GHz 35
nx9500-6C8809(config-smart-rf-policy-test)#

```

### Related Commands

|                 |                                               |
|-----------------|-----------------------------------------------|
| no on page 1650 | Disables recovery from faulty neighbor radios |
|-----------------|-----------------------------------------------|

### select-shutdown

This feature enables auto-shutdown of select 2.4 GHz radios, in dual-band networks, to maintain CCI (co-channel interference) levels within specified limits. When enabled, Smart-RF monitors CCI levels to ensure that the deployment average CCI remains within specified minimum and maximum CCI limits. If the deployment average CCI is found to exceed the maximum threshold value, 2.4 GHz radios, causing neighbor interference, are shut down one-by-one until the deployment average CCI falls below the maximum threshold value. The reverse process occurs when the deployment average CCI falls below the minimum threshold value. In this scenario, previously disabled radios are one-by-one enabled until the deployed average CCI reaches acceptable levels.

Use this command to enable select-shutdown and configure the maximum and minimum CCI thresholds.

**Supported in the following platforms:**

- Access Points — , AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

**Syntax**

```
select-shutdown {cci-high-threshold/cci-low-threshold/frequency/frequency-limiter}
select-shutdown {cci-high-threshold <-85--55>}
select-shutdown {cci-low-threshold <-100--55>}
select-shutdown {frequency <0-3600>}
select-shutdown {frequency-limiter <1-1000>}
```

**Parameters**

```
select-shutdown {cci-high-threshold <-85--55>|cci-low-threshold <-100--55>|
frequency <0-3600>|frequency-limiter <1-1000>}
```

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| select-shutdown              | Enables auto-shutdown of selected 2.4 GHz radios to maintain the deployment average CCI levels within a specified range                                                                                                                                                                                                                                                                                                                                                   |
| cci-high-threshold <-85--55> | Optional. Configures the maximum CCI threshold <ul style="list-style-type: none"> <li>• &lt;-85--55&gt; – Specify a value from -85 - -55 dBm. The default value is -80 dBm.</li> </ul> <p><b>Note:</b> If not specified, the system uses the default value as the upper limit.</p>                                                                                                                                                                                        |
| cci-low-threshold <-100--55> | Optional. Configures the minimum CCI threshold <ul style="list-style-type: none"> <li>• &lt;-100--55&gt; – Specify a value from -100 - -55 dBm. The default value is -100 dBm.</li> </ul> <p><b>Note:</b> If not specified, the system uses the default value as the lower limit.</p>                                                                                                                                                                                     |
| frequency <0-3600>           | Configures the interval, in minutes, at which 2.4 GHz radios are selected for shut down. When the deployment average CCI exceeds the specified maximum threshold, Smart RF shuts down 2.4 GHz radios until the CCI reaches acceptable levels. Use this option, to configure the interval between successive radio shut down. <ul style="list-style-type: none"> <li>• &lt;0-3600&gt; – Specify the frequency from 0 - 3600 minutes. The default is 60 minutes.</li> </ul> |
| frequency-limiter <1-1000>   | Configures the minimum multiple of Interference Recovery frequency that the select-shutdown frequency can be set to <ul style="list-style-type: none"> <li>• &lt;1-100&gt; – Specify a value from 1 - 1000. The default value is 15.</li> </ul>                                                                                                                                                                                                                           |



## Examples

```
nx9500-6C8809(config-smart-rf-policy-testSmartRF)#select-shutdown
cci-high-threshold -55
nx9500-6C8809(config-smart-rf-policy-testSmartRF)#select-shutdown
cci-low-threshold -95
nx9500-6C8809(config-smart-rf-policy-test)#show context
smart-rf-policy test
 group-by floor
 sensitivity custom
 assignable-power 2.4GHz max 20
 assignable-power 2.4GHz min 8
 channel-list 2.4GHz 1,12
 channel-width 5GHz auto
 channel-width 2.4GHz auto
 area test channel-list 2.4GHz 1,2,3
 avoidance-time dfs 300
 interference-recovery channel-switch-delta 2.4GHz 5
 neighbor-recovery power-threshold 5GHz -65
 neighbor-recovery power-threshold 2.4GHz -82
 select-shutdown cci-high-threshold -55
 select-shutdown cci-low-threshold -95
 coverage-hole-recovery snr-threshold 2.4GHz 35
nx9500-6C8809(config-smart-rf-policy-test)#
```

## Related Commands

`no` on page 1650

Disables select-shutdown of 2.4 GHz radios and reverts the select-shutdown parameters (maximum and minimum CCI thresholds, frequency, and frequency-limiter) to default values.

### *sensitivity*

Configures Smart RF sensitivity level. The sensitivity level determines Smart RF scanning and sampling aggressiveness. For example, a low sensitivity level indicates a less aggressive Smart-RF policy. This translates to fewer samples taken during off-channel scanning and short off-channel durations. When the sensitivity level is set to high, Smart-RF collects more samples, and remains off-channel longer.

The Smart RF sensitivity level options include **low**, **medium**, **high**, and **custom**. The custom option allows you to adjust the parameters and thresholds for interference recovery, coverage hole recovery, and neighbor recovery. However, the low, medium, and high settings still allow utilization of these features.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
sensitivity [custom|high|low|medium]
```

### Parameters

```
sensitivity [custom|high|low|medium]
```

|             |                                                                                                                    |
|-------------|--------------------------------------------------------------------------------------------------------------------|
| sensitivity | Configures Smart RF sensitivity levels. The options available are: custom, high, low, and medium.                  |
| custom      | Enables custom interference recovery, coverage hole recovery, and neighbor recovery as additional Smart RF options |
| high        | High sensitivity                                                                                                   |
| low         | Low sensitivity                                                                                                    |
| medium      | Medium sensitivity. This is the default setting.                                                                   |

### Usage Guidelines

To enable the *power* and *channel setting* parameters, set *sensitivity* to *custom* or *medium*.

To enable the *monitoring* and *scanning* parameters, set *sensitivity* to *custom*.

To enable the *neighbor recovery*, *interference* and *coverage hole recovery* parameters, set *sensitivity* to *custom*.

### Examples

```

nx9500-6C8809(config-smart-rf-policy-test)#sensitivity high
nx9500-6C8809(config-smart-rf-policy-test)#show context
smart-rf-policy test
 area test channel-list 2.4GHz 1,2,3
 group-by floor
 sensitivity high
 channel-list 2.4GHz 1,12
 channel-width 5GHz auto
 smart-ocs-monitoring frequency 5GHz 3
 smart-ocs-monitoring frequency 2.4GHz 3
 smart-ocs-monitoring sample-count 5GHz 3
 smart-ocs-monitoring sample-count 2.4GHz 3
 --More--
nx9500-6C8809(config-smart-rf-policy-test)#

```

#### *smart-ocs-monitoring*

Applies smart OCS (Off-Channel Scanning) instead of dedicated detectors

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
smart-ocs-monitoring {awareness-override/client-aware/extended-scan-frequency/
frequency/off-channel-duration/power-save-aware/sample-count/tx-load-aware/voice-aware}
smart-ocs-monitoring {awareness-override [schedule/threshold]}
smart-ocs-monitoring {awareness-override schedule <1-3> <START-TIME> <END-TIME> <DAY>}
smart-ocs-monitoring {awareness-override threshold <10-10000>}
smart-ocs-monitoring {client-aware [2.4GHz/5GHz] <1-255>}
smart-ocs-monitoring {extended-scan-frequency [2.4GHz/5GHz] <0-50>}
smart-ocs-monitoring {frequency [2.4GHz/5GHz] <1-120>}
smart-ocs-monitoring {off-channel-duration [2.4GHz/5GHz] <20-150>}
smart-ocs-monitoring {power-save-aware [2.4GHz/5GHz] [disable/dynamic/strict]}
smart-ocs-monitoring {sample-count [2.4GHz/5GHz] <1-15>}
smart-ocs-monitoring {tx-load-aware [2.4GHz/5GHz] <1-100>}
smart-ocs-monitoring {voice-aware [2.4GHz/5GHz] [disable/dynamic/strict]}
```

## Parameters

```
smart-ocs-monitoring {awareness-override schedule <1-3> <START-TIME> <END-TIME> <DAY>}
```

|                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| awareness-override                             | Optional. Use this parameter to configure client awareness settings overrides                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| schedule <1-3> <START-TIME> <END-TIME> {<DAY>} | <p>Configures a time and day schedule when awareness settings are overridden</p> <ul style="list-style-type: none"><li>• &lt;1-3&gt; - Sets the awareness override schedule index. A maximum of three overrides can be configured.</li><li>• &lt;START-TIME&gt; - Sets the override start time in HH:MM format</li><li>• &lt;END-TIME&gt; - Sets the override end time in HH:MM format</li></ul> <p>DAY - Optional. Set the day when the override is active. Use one of the following formats:</p> <ul style="list-style-type: none"><li>all - Override is active on all days</li><li>sun - Override is active only on Sundays</li><li>mon - Override is active only on Mondays</li><li>tue - Override is active only on Tuesdays</li><li>wed - Override is active only on Wednesdays</li><li>thu - Override is active only on Thursdays</li><li>fri - Override is active only on Fridays</li><li>sat - Override is active only on Saturdays</li></ul> |

```
smart-ocs-monitoring {awareness-override threshold <10-10000>}
```

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| awareness-override threshold <10-10000> | <p>Optional. Use this parameter to configure client awareness settings overrides</p> <ul style="list-style-type: none"><li>• threshold - Specifies the threshold after which client awareness settings are overridden. When the specified threshold is reached, awareness settings are overridden.</li><li>• &lt;10-10000&gt; - Specify a threshold value from 10 -10000. The default is 10.</li></ul> |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
smart-ocs-monitoring {client-aware [2.4GHz/5GHz] <1-255>}
```

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| client-aware      | Optional. Enables client aware scanning on this Smart RF policy<br>Use this parameter to configure a client threshold number. When the number of clients connected to a radio equals this threshold number,<br>Use this parameter to configure a client threshold number. When the number of clients connected to a radio equals the specified threshold, the radio avoids channel scanning. The radio does not change channel even if needed (based on the interference recovery determination made by the smart master).<br>This feature is disabled by default. |
| 2.4GHz<br><1-255> | Enables client aware scanning on the 2.4 GHz band<br>Avoids radio scanning when a specified minimum number of clients are present <ul style="list-style-type: none"> <li>• &lt;1-255&gt; - Sets the minimum number of clients from 1 - 255. The default is 50 clients.</li> </ul>                                                                                                                                                                                                                                                                                  |
| 5GHz<br><1-255>   | Enables client aware scanning on the 5.0 GHz band<br>Avoids radio scanning when a specified minimum number of clients are present <ul style="list-style-type: none"> <li>• &lt;1-255&gt; - Sets the minimum number of clients from 1 - 255. The default is 50 clients.</li> </ul>                                                                                                                                                                                                                                                                                  |

`smart-ocs-monitoring {extended-scan-frequency [2.4GHz|5GHz] <0-50>}`

|                         |                                                                                                                                                                       |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| extended-scan-frequency | Optional. Enables an extended scan, as opposed to a neighbor only scan, on this Smart RF policy. This is the frequency radios use to scan for non-peer radios.        |
| 2.4GHz <0-50>           | Enables extended scan on the 2.4 GHz band <ul style="list-style-type: none"> <li>• &lt;0-50&gt; - Sets the number of trails from 0 - 50. The default is 5.</li> </ul> |
| 5GHz <0-50>             | Enables extended scan on the 5.0 GHz band <ul style="list-style-type: none"> <li>• &lt;0-50&gt; - Sets the number of trails from 0 - 50. The default is 5.</li> </ul> |

`smart-ocs-monitoring {frequency [2.4GHz|5GHz] <1-120>}`

|                |                                                                                                                                                                    |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| frequency      | Optional. Specifies the scan frequency. This is the frequency, in seconds, in which smart-ocs-monitoring changes channels for an off-channel scan.                 |
| 2.4GHz <1-120> | Selects the 2.4 GHz band <ul style="list-style-type: none"> <li>• &lt;1-120&gt; - Sets a scan frequency from 1 sec - 120 sec. The default is 6 seconds.</li> </ul> |
| 5GHz <1-120>   | Selects the 5.0 GHz band <ul style="list-style-type: none"> <li>• &lt;1-120&gt; - Sets a scan frequency from 1 sec - 120 sec. The default is 6 seconds.</li> </ul> |

`smart-ocs-monitoring {off-channel-duration [2.4GHz|5GHz] <20-150>}`

|                      |                                                                                                                                                                                                                                                                                                                             |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| off-channel-duration | Optional. Specifies the duration to scan off channel<br>This is the duration for which an access point radio remains off-channel. During this period the radio monitors devices within the network and, if necessary, perform self healing and neighbor recovery to compensate for coverage area losses within a RF Domain. |
| 2.4GHz<br><20-150>   | Selects the 2.4 GHz band (in milliseconds) <ul style="list-style-type: none"> <li>• &lt;20-150&gt; - Sets the off channel duration from 20 - 150 milliseconds. The default is 50 milliseconds.</li> </ul>                                                                                                                   |
| 5GHz <20-150>        | Selects the 5.0 GHz band (in milliseconds) <ul style="list-style-type: none"> <li>• &lt;20-150&gt; - Sets the off channel duration from 20 - 150 milliseconds. The default is 50 milliseconds.</li> </ul>                                                                                                                   |

`smart-ocs-monitoring {power-save-aware [2.4GHz|5GHz] [disable|dynamic|strict]}`

|                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| power-save-aware                           | Optional. Enables power save awareness scanning mode on this Smart RF policy. The options are: disable, dynamic, and strict.<br>This setting allows Smart RF to detect power save clients and take them into consideration when performing off channel scans.<br>Strict disables smart monitoring as long as a power save capable client is associated to a radio.<br>Dynamic disables smart monitoring as long as there is data buffered for a power save client at the radio. |
| 2.4GHz<br>[disable <br>dynamic <br>strict] | Sets power save aware scanning mode on the 2.4 GHz band <ul style="list-style-type: none"> <li>• disable – Disables voice awareness scanning</li> <li>• dynamic – Dynamically avoids scanning based on traffic for power save (PSP) clients. This is the default setting.</li> <li>• strict – Strictly avoids scanning when PSP clients are present</li> </ul>                                                                                                                  |
| 5GHz [disable <br>dynamic <br>strict]      | Sets power save aware scanning mode on the 5.0 GHz band <ul style="list-style-type: none"> <li>• disable – Disables voice awareness .scanning</li> <li>• dynamic – Dynamically avoids scanning based on traffic for PSP clients. This is the default setting.</li> <li>• strict – Strictly avoids scanning when voice PSP are present</li> </ul>                                                                                                                                |

```
smart-ocs-monitoring {sample-count [2.4GHz|5GHz] <1-15>}
```

|               |                                                                                                                                                                       |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| sample-count  | Optional. Specifies the number of samples to collect before reporting an issue to the Smart RF master                                                                 |
| 2.4GHz <1-15> | Selects the 2.4 GHz band <ul style="list-style-type: none"> <li>• &lt;1-15&gt; – Specifies the number of samples to collect from 1 - 15. The default is 10</li> </ul> |
| 5GHz <1-15>   | Selects the 5.0 GHz band <ul style="list-style-type: none"> <li>• &lt;1-15&gt; – Specifies the number of samples to collect from 1 - 15. The default is 5.</li> </ul> |

```
smart-ocs-monitoring {tx-load-aware [2.4GHz|5GHz] <1-100>}
```

|                |                                                                                                                                                                                                                 |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| tx-load-aware  | Optional. Specifies a transmit load percentage that serves as a threshold before scanning is avoided for an access point's 2.4 GHz or 5.0 GHz band. This option is disabled for both 2.4 GHz and 5.0 GHz bands. |
| 2.4GHz <1-100> | Selects the 2.4 GHz band <ul style="list-style-type: none"> <li>• &lt;1-100&gt; – Specify a transmit load percentage from 1 - 100%. When enabled, the default is 1%.</li> </ul>                                 |
| 5GHz <1-100>   | Selects the 5.0 GHz band <ul style="list-style-type: none"> <li>• &lt;1-100&gt; – Specify a transmit load percentage from 1 - 100%. When enabled, the default is 1%.</li> </ul>                                 |

```
smart-ocs-monitoring {voice-aware [2.4GHz|5GHz] [disable|dynamic|strict]}
```

|                                  |                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| voice-aware                      | Optional. Enables voice awareness scanning mode on this Smart RF policy. The options are: <b>disable</b> , <b>dynamic</b> , and <b>strict</b> .<br>Strict disables smart monitoring as long as a voice client is associated to a radio. Dynamic disables smart monitoring as long as there is data buffered for a voice client at the radio.  |
| 2.4GHz [disable] dynamic strict] | Specifies the scanning mode on the 2.4 GHz band <ul style="list-style-type: none"> <li>• disable – Disables voice awareness scanning</li> <li>• dynamic – Dynamically avoids scanning based on traffic for voice clients. This is the default setting.</li> <li>• strict – Strictly avoids scanning when voice clients are present</li> </ul> |
| 5GHz [dynamic] strict]           | Specifies the scanning mode on the 5.0 GHz band <ul style="list-style-type: none"> <li>• dynamic – Dynamically avoids scanning based on traffic for voice clients. This is the default setting.</li> <li>• strict – Strictly avoids scanning when voice clients are present.</li> </ul>                                                       |

### Examples

```

nx9500-6C8809(config-smart-rf-policy-test)#smart-ocs-monitoring extended-scan-frequency
2.4GHz 9
nx9500-6C8809(config-smart-rf-policy-test)#smart-ocs-monitoring awareness-override
schedule 1 12:30 20:30
nx9500-6C8809(config-smart-rf-policy-test)#show context
smart-rf-policy test
 group-by floor
 sensitivity custom
 assignable-power 2.4GHz max 20
 assignable-power 2.4GHz min 8
 channel-list 2.4GHz 1,12
 channel-width 5GHz auto
 channel-width 2.4GHz auto
 area test channel-list 2.4GHz 1,2,3
 avoidance-time dfs 300
 no smart-ocs-monitoring
 smart-ocs-monitoring frequency 5GHz 3
 smart-ocs-monitoring frequency 2.4GHz 3
 smart-ocs-monitoring sample-count 5GHz 3
 smart-ocs-monitoring extended-scan-frequency 5GHz 0
 smart-ocs-monitoring extended-scan-frequency 2.4GHz 9
 smart-ocs-monitoring awareness-override schedule 1 12:30 20:30 all
 interference-recovery client-threshold 255
 interference-recovery channel-switch-delta 5GHz 5
--More--
nx9500-6C8809(config-smart-rf-policy-test)#

```

### Related Commands

|                              |                                 |
|------------------------------|---------------------------------|
| <code>no</code> on page 1650 | Disables off-channel monitoring |
|------------------------------|---------------------------------|

*no*

Negates a command or sets its default. When used in the config Smart RF policy mode, the `no` command disables or resets Smart RF settings.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533

- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
no [area|assignable-power|avoidance-time|channel-list|channel-width|coverage-hole-recovery|
enable|group-by|interference-recovery|neighbor-recovery|select-shutdown|smart-ocs-
monitoring]
no area <AREA-NAME> channel-list [2.4GHZ|5GHZ]
no assignable-power [2.4GHZ|5GHZ] [max|min]
no [channel-list|channel-width] [2.4GHZ|5GHZ]
no coverage-hole-recovery [client-threshold|coverage-interval|interval|snr-threshold]
[2.4GHZ|5GHZ]
no avoidance-time [adaptivity|dfs]
no enable
no group-by [area|floor]
no interference-recovery {channel-hold-time|channel-switch-delta [2.4GHZ|5GHZ]|
client-threshold|interference|neighbor-offset|noise|noise-factor}
no neighbor-recovery {dynamic-sampling {retries|threshold}|power-hold-time|power-threshold
[2.4GHZ|5GHZ]}
no select-shutdown {cci-high-threshold|cci-low-threshold|frequency|frequency-limiter}
no smart-rf-monitoring {awareness-override [schedule <1-3>|threshold]|client-aware [2.4GHZ|
5GHZ]}
extended-scan-frequency [2.4GHZ|5GHZ]|frequency [2.4GHZ|5GHZ]|off-channel-duration [2.4GHZ|
5GHZ]|
power-save-aware [2.4GHZ|5GHZ]|sample-count [2.4GHZ|5GHZ]|voice-aware [2.4GHZ|5GHZ]}
```

## Parameters

no <PARAMETERS>

no <PARAMETERS> Negates a command or sets its default. When used in the config Smart RF policy mode, the no command disables or resets the Smart RF policy settings.

## Examples

The following example shows the Smart RF policy 'test' settings before the 'no' commands are executed:

```
nx9500-6C8809(config-smart-rf-policy-test)#show context
smart-rf-policy test
 group-by floor
 sensitivity custom
 assignable-power 2.4GHz max 20
 assignable-power 2.4GHz min 8
 channel-list 2.4GHz 1,12
 channel-width 5GHz auto
 channel-width 2.4GHz auto
 area test channel-list 2.4GHz 1,2,3
 avoidance-time dfs 300
 no smart-ocs-monitoring
 smart-ocs-monitoring frequency 5GHz 3
 smart-ocs-monitoring frequency 2.4GHz 3
 smart-ocs-monitoring sample-count 5GHz 3
 smart-ocs-monitoring extended-scan-frequency 5GHz 0
 smart-ocs-monitoring extended-scan-frequency 2.4GHz 9
 smart-ocs-monitoring awareness-override schedule 1 12:30 20:30 all
 interference-recovery client-threshold 255
 interference-recovery channel-switch-delta 5GHz 5
 interference-recovery channel-switch-delta 2.4GHz 5
 neighbor-recovery power-threshold 5GHz -65
 neighbor-recovery power-threshold 2.4GHz -65
 select-shutdown CCI high threshold -82
```

```

select-shutdown CCI low threshold -95
select-shutdown frequency 30
select-shutdown frequency-limiter 5
coverage-hole-recovery interval 5GHz 15
coverage-hole-recovery interval 2.4GHz 15
coverage-hole-recovery coverage-interval 5GHz 5
coverage-hole-recovery coverage-interval 2.4GHz 5
interference-recovery channel-hold-time 180
nx9500-6C8809(config-smart-rf-policy-test)#
nx9500-6C8809(config-smart-rf-policy-test)#no interference-recovery channel-switch-delta
5GHz
nx9500-6C8809(config-smart-rf-policy-test)#no neighbor-recovery power-threshold 2.4GHz
nx9500-6C8809(config-smart-rf-policy-test)#no neighbor-recovery power-threshold 5GHz
nx9500-6C8809(config-smart-rf-policy-test)#no assignable-power 2.4GHz min
nx9500-6C8809(config-smart-rf-policy-test)#no assignable-power 5GHz max

```

The following example shows the Smart RF policy 'test' settings after the 'no' commands are executed:

```

nx9500-6C8809(config-smart-rf-policy-test)#show context
smart-rf-policy test
 group-by floor
 sensitivity custom
 channel-list 2.4GHz 1,12
 channel-width 5GHz auto
 channel-width 2.4GHz auto
 area test channel-list 2.4GHz 1,2,3
 avoidance-time dfs 300
 no smart-ocs-monitoring
 smart-ocs-monitoring frequency 5GHz 3
 smart-ocs-monitoring frequency 2.4GHz 3
 smart-ocs-monitoring sample-count 5GHz 3
 smart-ocs-monitoring extended-scan-frequency 5GHz 0
 smart-ocs-monitoring extended-scan-frequency 2.4GHz 9
 smart-ocs-monitoring awareness-override schedule 1 12:30 20:30 all
 interference-recovery client-threshold 255
 interference-recovery channel-switch-delta 2.4GHz 5
 select-shutdown CCI high threshold -82
 select-shutdown CCI low threshold -95
 select-shutdown frequency 30
 select-shutdown frequency-limiter 5
 coverage-hole-recovery interval 5GHz 15
 coverage-hole-recovery interval 2.4GHz 15
 coverage-hole-recovery coverage-interval 5GHz 5
 coverage-hole-recovery coverage-interval 2.4GHz 5
 interference-recovery channel-hold-time 180
nx9500-6C8809(config-smart-rf-policy-test)#

```



# WIPS POLICY

## WIPS-POLICY

---

This chapter summarizes the WIPS (Wireless Intrusion Protection Systems) policy commands in the CLI command structure.

WIPS is an additional measure of security designed to continuously monitor the network for threats and intrusions. Along with wireless VPNs, encryptions, and authentication policies WIPS enhances the security of a WLAN.

The WIPS policy enables detection of intrusions and threats that a managed network is likely to encounter. However, the WIPS policy does not include threat mitigation configurations. These intrusions and threats are available within the WIPS policy configuration mode as pre configured, fixed events. Each event consists of a set of frames or anomalies that may be harmful to the managed network. You can enable/disable various aspects of each individual event.

Events are broadly grouped into the following three categories:

- **Excessive/Thresholdable events:** These events detect DOS attacks, like excessive deauths, EAP floods, etc. Threshold limits for such events can be configured for MUs (mobile units) and radios. Once these threshold limits are exceeded, an event is triggered. Stations triggering an event are usually filtered. You can configure a filter ageout specifying the time for which the station, triggering the event, is filtered. However, the filter ageout only applies when the MU-threshold is exceeded. When radio threshold is reached, the system raises a warning about the same and updates event history with event details.
- **Station/MU anomalies:** These events are triggered when a MU performs suspicious activities that can compromise the security and stability of the managed network. You can configure a filter ageout, similar to the above class of events, to filter the station triggering such events.
- **AP/neighbor anomalies:** These events are triggered when an AP or neighbor sends suspicious frames. The system cannot filter APs or neighbors triggering such events. However, the system warns you about such attacks, allowing you to take further actions against such APs and neighbors.

In addition to event monitoring configuration, the WIPS policy allows you to configure a list of signatures. Unlike events, signatures are not fixed. You are free to define your own signatures based on a specific set of parameters. A signature is a rule, consisting of a set of fields to match and a corresponding set of actions in case of a match. By default, whenever a signature is matched an event log is triggered. This event log is similar to the one triggered upon an event. In addition to an event log, you can also configure other actions. Signatures have all the features supported by events. In fact most events are internally implemented as signatures.

Signature rules are of the following three types:

- **ssid, ssid length rule:** This signature matches a specified SSID or SSID length. It is mandatory to configure the frame type to match for this signature. When configured, only frame types allowed are beacons, probe requests, and probe responses. Example rule: `ssid : AirJack and frame type beacon` : Signature for AirJack attack.

- payload rule: This signature matches a particular payload at a particular frame offset. You can restrict these matches based on frame type. Example rule: Payload : 0x00601d Offset 3 : Netstumbler
- address-match rule: This signature matches one or more address fields. The address fields supported are BSSID, source-MAC, and destination-MAC. You can also specify frame types to match. The frame types supported are assoc, auth, beacon, data, death, disassoc, mgmt, probe-request, and probe-response.

A WIPS policy, once configured, has to be attached to a RF Domain to take effect. Multiple WIPS policies can be configured at the same time, but only one policy can be attached to a given RF Domain at any time.



#### Note

To attach a WIPS policy to a RF Domain, in the RF Domain configuration mode, execute the **use > wips-policy <WIPS-POLICY-NAME>** command. For more information, [use \(rf-domain-config-mode\)](#) on page 524.



#### Note

With this most recent release, AP 7522 and AP 7532 model access points can provide enhanced sensor support. AP 7522 and AP 7532 sensors can send data from off-channel-scans while in radio-share promiscuous/inline mode, in addition to the on-channel data captured in radio-share mode. ADSP uses the off-channel-scan data (in addition to the on-channel data) to monitor for rogue intrusions and trigger alarms. OTA Termination is triggered from ADSP to the appropriate radio-share AP to initiate termination.



#### Note

AP 7522 and AP 7532 models also support shared part-time scanning using WIPS in WiNG (using off-channel-scans) and no ADSP. WIPS on WiNG was enhanced to add rogue detection/classification (wired side detection based of MAC Address Offset) and OTA (over-the-air) termination for AP 7522 and AP 7532 deployments.

Use the (config) instance to configure WIPS policy commands. To navigate to the WIPS policy instance, use the following commands:

```
<DEVICE>(config)#wips-policy <POLICY-NAME>
nx9500-6C8809(config)#wips-policy test
nx9500-6C8809(config-wips-policy-test)#?
Wips Policy Mode commands:
 ap-detection Rogue AP detection
 enable Enable this wips policy
 event Configure an event
 history-throttle-duration Configure the duration for which event duplicates
 are not stored in history
 interference-event Specify events which will contribute to smart-rf
 wifi interference calculations
 no Negate a command or set its defaults
 signature Signature to configure
 use Set setting to use
 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
```

```

service Service Commands
show Show running system information
write Write running configuration to memory or terminal

```

```
nx9500-6c8809(config-wips-policy-test)#
```

## wips-policy-commands

The following table summarizes WIPS policy configuration commands:

Table: WIPS-Policy Config Mode Commands

| Command                                                | Description                                                                  |
|--------------------------------------------------------|------------------------------------------------------------------------------|
| <a href="#">ap-detection</a> on page 1655              | Defines the WIPS AP detection configuration                                  |
| <a href="#">enable</a> on page 1657                    | Enables the WIPS policy                                                      |
| <a href="#">event</a> on page 1657                     | Configures events                                                            |
| <a href="#">history-throttle-duration</a> on page 1660 | Configures the duration event duplicates are omitted from the event history  |
| <a href="#">interference-event</a> on page 1661        | Specifies events contributing to the Smart RF WiFi interference calculations |
| <a href="#">signature</a> on page 1662                 | Configures a WIPS policy signature and enters its configuration mode         |
| <a href="#">use</a> on page 1673                       | Defines a WIPS policy settings                                               |
| <a href="#">no</a> on page 1672                        | Negates a command or sets its default                                        |



### Note

For more information on common commands (clrcr, commit, help, revert, service, show, write, and exit), see [COMMON COMMANDS](#) on page 640.



### Note

The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (\_) character. In other words, the name of a device cannot contain an underscore.

### *ap-detection*

Enables the detection of unauthorized or unsanctioned APs. Unauthorized APs are untrusted access points connected to an access point managed network. These untrusted APs accept wireless client associations. It is important to detect such rogue APs and declare them unauthorized. Rogue AP detection is disabled by default.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
ap-detection {ageout/air-termination/interferer-threshold/recurring-event-interval/wait-time}
ap-detection {ageout <30-86400>/interferer-threshold <-100--10>/recurring-event-interval <0-10000>/wait-time <10-600>}
ap-detection air-termination {allow-channel-switch/mode [auto/manual]}
```

## Parameters

```
ap-detection {ageout <30-86400>/interferer-threshold <-100--10>/recurring-event-interval <0-10000>/wait-time <10-600>}
```

|                                    |                                                                                                                                                                                                                                                                                   |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ap-detection                       | Enables detection of unauthorized or unsanctioned APs                                                                                                                                                                                                                             |
| ageout <30-86400>                  | Optional. Configures the unauthorized AP ageout interval. The WIPS policy uses this value to ageout unauthorized APs. <ul style="list-style-type: none"><li>&lt;30-86400&gt; - Sets an ageout interval from 30 - 86400 seconds. The default is 5 minutes (300 seconds).</li></ul> |
| recurring-event-interval <0-10000> | Configures recurring event interval help of unauthorized APs <ul style="list-style-type: none"><li>&lt;0-10000&gt; - Configures the recurring interval between 0 - 10000 seconds. The default is 300 seconds.</li></ul>                                                           |
| interferer-threshold <-100--10>    | Configures RSSI threshold value to determine if an unsanctioned ap is an interferer or not <ul style="list-style-type: none"><li>&lt;-100--10&gt; - Configures the rssi threshold between -100 - -10 dBm. The default is -75 dBm.</li></ul>                                       |
| wait-time <10-600>                 | Optional. Configures the wait time before a detected AP is declared as unauthorized and potentially removed <ul style="list-style-type: none"><li>&lt;10-600&gt; - Sets a wait time from 10 - 600 seconds. The default is 1 minute (60 seconds).</li></ul>                        |

```
ap-detection air-termination {allow-channel-switch/mode [auto/manual]}
```

|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ap-detection                                               | Enables detection of unauthorized or unsanctioned APs                                                                                                                                                                                                                                                                                                                                                          |
| air-termination {allow-channel-switch} mode [auto/manual]} | Enables air termination of unauthorized APs. This option is disabled by default. <ul style="list-style-type: none"><li>allow-channel-switch - Optional. Allows channel switch of unauthorized APs based on the channel mode. This option is disabled by default.</li><li>mode [auto/manual] - Optional. Select the mode as <b>auto</b> or <b>manual</b> to configure. The default setting is manual.</li></ul> |

## Examples

```
nx9500-6C8809(config-wips-policy-test)#ap-detection wait-time 15
nx9500-6C8809(config-wips-policy-test)#ap-detection age-out 50
nx9500-6C8809(config-wips-policy-test)#show context
wips-policy test
 ap-detection-age-out 50
 ap-detection-wait-time 15
nx9500-6C8809(config-wips-policy-test)#
nx9500-6C8809(config-wips-policy-test2)#ap-detection recurring-event-interval 10
nx9500-6C8809(config-wips-policy-test2)#show context
wips-policy test2
 ap-detection recurring-event-interval 10
nx9500-6C8809(config-wips-policy-test2)#
```

## Related Commands

|                              |                                                                      |
|------------------------------|----------------------------------------------------------------------|
| <code>no</code> on page 1672 | Resets unauthorized or unsanctioned AP detection settings to default |
|------------------------------|----------------------------------------------------------------------|

### *enable*

Enables this WIPS policy

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

`enable`

#### Parameters

None

#### Examples

```
nx9500-6C8809(config-wips-policy-test)#enable
```

## Related Commands

|                              |                          |
|------------------------------|--------------------------|
| <code>no</code> on page 1672 | Disables the WIPS policy |
|------------------------------|--------------------------|

### *event*

Configures events, filters and threshold values for this WIPS policy. Events are grouped into three categories, AP anomaly, client anomaly, and excessive. WLANs are baselined for matching criteria. Any deviation from this baseline is considered an anomaly and logged as an event.



#### Note

By default all event monitoring is disabled.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
event [ap-anomaly|client-anomaly|enable-all-events|excessive]
event ap-anomaly [ad-hoc-violation|airjack|ap-ssid-broadcast-in-beacon|asleep|
impersonation-attack|null-probe-response|transmitting-device-using-invalid-mac|
unencrypted-wired-leakage|wireless-bridge]
event client-anomaly [dos-broadcast-deauth|fuzzing-all-zero-macs|
fuzzing-invalid-frame-type|fuzzing-invalid-mgmt-frames|fuzzing-invalid-seq-num|
```

```

identical-src-and-dest-addr|invalid-8021x-frames|netstumbler-generic|
non-conforming-data|wellenreiter] {filter-ageout <0-86400>}
event enable-all-events
event excessive [80211-replay-check-failure|aggressive-scanning|auth-server-failures|
decryption-failures|dos-assoc-or-auth-flood|dos-eapol-start-storm|dos-unicast-deauth-or-
disassoc|
eap-flood|eap-nak-flood|frames-from-unassoc-station] {filter-ageout <0-86400>/
threshold-client <0-65535>/threshold-radio <0-65535>}

```

## Parameters

```

event ap-anomaly [ad-hoc-violation|airjack|ap-ssid-broadcast-in-beacon|asleep|
impersonation-attack|null-probe-response|transmitting-device-using-invalid-mac|
unencrypted-wired-leakage|wireless-bridge]

```

|                                       |                                                                                                                                                                                                                                                                       |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ap-anomaly                            | Enables AP anomaly event tracking<br>An AP anomaly event refers to suspicious frames sent by neighboring APs. An administrator enables or disables the filtering of each listed event and sets the thresholds for the generation of event notification and filtering. |
| ad-hoc-violation                      | Tracks ad-hoc network violations                                                                                                                                                                                                                                      |
| airjack                               | Tracks AirJack attacks                                                                                                                                                                                                                                                |
| ap-ssid-broadcast-in-beacon           | Tracks AP SSID broadcasts in beacon events                                                                                                                                                                                                                            |
| asleep                                | Tracks ASLEAP attacks. These attacks break LEAP (Lightweight Extensible Authentication Protocol) passwords                                                                                                                                                            |
| impersonation-attack                  | Tracks impersonation attacks. These are also referred to as spoofing attacks, where the attacker assumes the address of an authorized device.                                                                                                                         |
| null-probe-response                   | Tracks null probe response attacks                                                                                                                                                                                                                                    |
| transmitting-device-using-invalid-mac | Tracks the transmitting device using an invalid MAC address                                                                                                                                                                                                           |
| unencrypted-wired-leakage             | Tracks unencrypted wired leakage                                                                                                                                                                                                                                      |
| wireless-bridge                       | Tracks WDS (wireless bridge) frames                                                                                                                                                                                                                                   |

```

event client-anomaly [dos-broadcast-deauth|fuzzing-all-zero-macs|fuzzing-invalid-frame-
type|
fuzzing-invalid-mgmt-frames|fuzzing-invalid-seq-num|identical-src-and-dest-addr|
invalid-8021x-frames|
netstumbler-generic|non-conforming-data|wellenreiter] {filter-ageout <0-86400>}

```

|                             |                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| client-anomaly              | Enables client anomaly event tracking<br>These are suspicious events performed by wireless clients that compromising the security of the network. An administrator can enable or disable the filtering of each listed event and set the thresholds required for the generation of the event notification and filtering action applied. |
| dos-broadcast-deauth        | Tracks DoS broadcast deauthentication events                                                                                                                                                                                                                                                                                           |
| fuzzing-all-zero-macs       | Tracks Fuzzing: All zero MAC addresses observed                                                                                                                                                                                                                                                                                        |
| fuzzing-invalid-frame-type  | Tracks Fuzzing: Invalid frame type detected                                                                                                                                                                                                                                                                                            |
| fuzzing-invalid-mgmt-frames | Tracks Fuzzing: Invalid management frame detected                                                                                                                                                                                                                                                                                      |
| fuzzing-invalid-seq-num     | Tracks Fuzzing: Invalid sequence number detected                                                                                                                                                                                                                                                                                       |

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| identical-src-and-dest-addr | Tracks identical source and destination addresses detection                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| invalid-8021x-frames        | Tracks Fuzzing: Invalid 802.1x frames detected                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| netstumbler-generic         | Tracks Netstumbler (v3.2.0, 3.2.3, 3.3.0) events                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| non-changing-wep-iv         | Tracks unchanging WEP IV events                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| non-conforming-data         | Tracks non conforming data packets                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| wellenreiter                | Tracks Wellenreiter events                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| filter-ageout <0-86400>     | <p>The following keywords are common to all of the above client anomaly events:</p> <ul style="list-style-type: none"> <li>filter-ageout &lt;0-86400&gt; – Optional. Configures the filter expiration time in seconds</li> <li>&lt;0-86400&gt; – Sets the filter ageout time from 0 - 86400 seconds. The default is 0 seconds.</li> </ul> <p><b>Note:</b> For each violation define a filter time in seconds, which determines how long the packets (received from an attacking device) are ignored once a violation has been triggered. Ignoring frames from an attacking device minimizes the effectiveness of the attack and the impact to the site until permanent mitigation can be performed.</p> <p>The filter ageout value is applicable across the entire RF Domain using this WIPS policy. If an MU is detected performing an attack and is filtered by one of the APs, the information is passed on to all APs and controllers within the RF Domain through the domain manager. Consequently the MU is filtered, for the specified period of time, across all devices.</p> |

event enable-all-events

|                   |                                                                                |
|-------------------|--------------------------------------------------------------------------------|
| enable-all-events | Enables tracking of all intrusion events (client anomaly and excessive events) |
|-------------------|--------------------------------------------------------------------------------|

```
event excessive [80211-replay-check-failure|aggressive-scanning|
auth-server-failures|decryption-failures|dos-assoc-or-auth-flood|dos-eapol-start-storm|
dos-unicast-deauth-or-disassoc|eap-flood|eap-nak-flood|frames-from-unassoc-station]
{filter-ageout [<0-86400>]|threshold-client [<0-5535>]|threshold-radio <0-65535>}
```

|                                |                                                                                                                                                                                                                                  |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| excessive                      | Enables the tracking of excessive events. Excessive events are actions performed continuously and repetitively. These events can impact the performance of the controller managed network. DoS attacks come under this category. |
| 80211-replay-check-failure     | Tracks 802.11replay check failure                                                                                                                                                                                                |
| aggressive-scanning            | Tracks aggressive scanning events                                                                                                                                                                                                |
| auth-server-failures           | Tracks failures reported by authentication servers                                                                                                                                                                               |
| decryption-failures            | Tracks decryption failures                                                                                                                                                                                                       |
| dos-assoc-or-auth-flood        | Tracks DoS association or authentication floods                                                                                                                                                                                  |
| dos-eapol-start-storm          | Tracks DoS EAPOL start storms                                                                                                                                                                                                    |
| dos-unicast-deauth-or-disassoc | Tracks DoS dissociation or deauthentication floods                                                                                                                                                                               |
| eap-flood                      | Tracks EAP floods                                                                                                                                                                                                                |
| eap-nak-flood                  | Tracks EAP NAK floods                                                                                                                                                                                                            |

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| frames-from-unassoc-station   | Tracks frames from unassociated clients                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| filter-ageout<br><0-86400>    | <p>The following keywords are common to all excessive events:</p> <ul style="list-style-type: none"> <li>filter-ageout &lt;0-86400&gt; – Optional. Configures a filter expiration time in seconds. It sets the duration for which the client is filtered. The client is added to a ACL as a special entry and frames received from this client are dropped.</li> <li>&lt;0-86400&gt; – Sets a filter ageout time from 0 - 86400 seconds. The default is 0 seconds.</li> </ul> <p><b>Note:</b> This value is applicable across the RF Domain. If a client is detected performing an attack and is filtered by one of the APs, the information is passed to the domain controller. The domain controller then propagates this information to all APs and wireless controllers in the RF Domain.</p> |
| threshold-client<br><0-65535> | <p>The following keywords are common to all excessive events:</p> <ul style="list-style-type: none"> <li>threshold-client &lt;0-65535&gt; – Optional. Configures a client threshold value after which the filter is triggered and an event is recorded</li> <li>&lt;0-65535&gt; – Sets a wireless client threshold value from 0 - 65535 seconds</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| threshold-radio<br><0-65535>  | <p>The following keywords are common to all excessive events:</p> <ul style="list-style-type: none"> <li>threshold-radio &lt;0-65535&gt; – Optional. Configures a radio threshold value after which the filter is triggered and an event is recorded</li> <li>&lt;0-65535&gt; – Sets a radio threshold value from 0 - 65535 seconds</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Examples

```

nx9500-6C8809(config-wips-policy-test)#event excessive 80211-replay-check-failure
filter-ageout 9 threshold-client 8 threshold-radio 99
nx9500-6C8809(config-wips-policy-test)#show context
wips-policy test
 event excessive 80211-replay-check-failure threshold-client 10 threshold-radio 99 filter-
ageout 9
 event client-anomaly wellenreiter filter-ageout 99
 ap-detection-ageout 50
 ap-detection-wait-time 15
nx9500-6C8809(config-wips-policy-test)#

```

## Related Commands

|                 |                                      |
|-----------------|--------------------------------------|
| no on page 1672 | Disables WIPS policy events tracking |
|-----------------|--------------------------------------|

### *history-throttle-duration*

Configures the duration event duplicates are omitted from the event history

The system maintains a history of all events that have occurred, on each device, within a RF Domain. Sometimes an event occurs for a prolonged period of time and tends to fill up the event history list. In such a scenario, duplicate information added to the event history list can be throttled for a specified period of time. Once this period is over, duplicate entries are once again allowed.

Event history statistics are periodically sent to the domain manager, which can be queried to ascertain the general health of the domain.



### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
history-throttle-duration <30-86400>
```

### Parameters

```
history-throttle-duration <30-86400>
```

|                           |                                                                                                                                        |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| history-throttle-duration | Configures the duration event duplicates are omitted from the event history <30-86400>                                                 |
|                           | <ul style="list-style-type: none"><li>• &lt;30-86400&gt; – Sets a value from 30 - 86400 seconds. The default is 120 seconds.</li></ul> |

### Examples

```
nx9500-6C8809(config-wips-policy-test)#history-throttle-duration 77
nx9500-6C8809(config-wips-policy-test)#show context
wips-policy test
 history-throttle-duration 77
 event excessive 80211-replay-check-failure threshold-client 10 threshold-radio 99 filter-ageout 9
 event client-anomaly wellenreiter filter-ageout 99
 ap-detection-ageout 50
 ap-detection-wait-time 15
nx9500-6C8809(config-wips-policy-test)#
```

### Related Commands

|                              |                                                                   |
|------------------------------|-------------------------------------------------------------------|
| <code>no</code> on page 1672 | Resets the history-throttle duration to its default (120 seconds) |
|------------------------------|-------------------------------------------------------------------|

### *interference-event*

Specifies events contributing to the Smart RF WiFi interference calculations

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
interference-event [non-conforming-data|wireless-bridge]
```

### Parameters

```
interference-event [non-conforming-data|wireless-bridge]
```

|                     |                                                                               |
|---------------------|-------------------------------------------------------------------------------|
| non-conforming-data | Considers non conforming data packets when calculating Smart RF interference  |
| wireless-bridge     | Considers Wireless Bridge (WDS) frames when calculating Smart RF interference |

## Examples

```
nx9500-6C8809(config-wips-policy-test)#interference-event non-conforming-data
nx9500-6C8809(config-wips-policy-test)#show context
wips-policy test
 history-throttle-duration 77
 event excessive 80211-replay-check-failure threshold-client 10 threshold-radio 99 filter-
ageout 9
 event client-anomaly wellenreiter filter-ageout 99
 interference-event non-conforming-data
 ap-detection-ageout 50
 ap-detection-wait-time 15
nx9500-6C8809(config-wips-policy-test)#
```

## Related Commands

|                              |                                                                     |
|------------------------------|---------------------------------------------------------------------|
| <code>no</code> on page 1672 | Disables this WIPS policy signature as Smart RF interference source |
|------------------------------|---------------------------------------------------------------------|

### *signature*

Configures a WIPS policy signature. A WIPS signature is the set of parameters or patterns used by WIPS to identify and categorize particular sets of attack behaviors in order to classify them. Use this option to configure signatures in the WIPS policy. The WIPS policy compares packets in the network with pre configured signatures to identify threats.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
signature <SIGNATURE-NAME>
```

## Parameters

```
signature <SIGNATURE-NAME>
```

|                            |                                                                                                                                                                  |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| signature <SIGNATURE-NAME> | Configures a WIPS policy signature                                                                                                                               |
|                            | <ul style="list-style-type: none"><li>• &lt;SIGNATURE-NAME&gt; - Enter a name for the WIPS policy signature. The name should not exceed 64 characters.</li></ul> |

## Examples

```
nx9500-6C8809(config-wips-policy-test)#signature test
nx9500-6C8809(config-test-signature-test)#
nx9500-6C8809(config-test-signature-test)#?
Wips Signature Mode commands:
 bssid Bssid mac address
 dst-mac Destination mac address
 filter-ageout Configure filter ageout
 frame-type Configure frame-type to match
 interference-event Signature is a smart-rf interference source
 mode Enable/Disable signature
 no Negate a command or set its defaults
 payload Configure a payload
 src-mac Source mac address
```

```

ssid-match Match based on ssid
threshold-client Configure client threshold limit
threshold-radio Configure radio threshold limit

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

```

```
nx9500-6C8809(config-test-signature-test)#
```

### Related Commands

|                                 |                                 |
|---------------------------------|---------------------------------|
| <a href="#">no</a> on page 1672 | Deletes a WIPS policy signature |
|---------------------------------|---------------------------------|

### signature mode commands

The following table summarizes WIPS policy signature configuration mode commands:

**Table 52: Table: WIPS-Policy-Signature Config Mode Commands**

| Commands                                        | Description                                                               |
|-------------------------------------------------|---------------------------------------------------------------------------|
| <a href="#">bssid</a> on page 1663              | Configures the BSSID MAC address                                          |
| <a href="#">dst-mac</a> on page 1664            | Configures the destination MAC address                                    |
| <a href="#">filter-ageout</a> on page 1664      | Configures the filter ageout interval                                     |
| <a href="#">frame-type</a> on page 1665         | Configures the frame type used for matching                               |
| <a href="#">interference-event</a> on page 1666 | Configures this WIPS policy signature as the Smart RF interference source |
| <a href="#">mode</a> on page 1667               | Enables the signature mode                                                |
| <a href="#">payload</a> on page 1667            | Configures payload settings                                               |
| <a href="#">src-mac</a> on page 1668            | Configures the source MAC address                                         |
| <a href="#">ssid-match</a> on page 1668         | Configures a match based on SSID                                          |
| <a href="#">threshold-client</a> on page 1669   | Configures the wireless client threshold limit                            |
| <a href="#">threshold-radio</a> on page 1670    | Configures the radio threshold limit                                      |
| <a href="#">no</a> on page 1671                 | Negates a command or sets its default                                     |

[bssid](#)

Configures a BSSID MAC address with this WIPS signature for matching

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533

- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

`bssid <MAC>`

#### Parameters

`bssid <MAC>`

`bssid <MAC>` Configures a BSSID MAC address for matching purposes and potential device exclusion

- `<MAC>` - Specify the MAC address.

#### Examples

```
nx9500-6C8809(config-test-signature-test)#bssid 11-22-33-44-55-66
nx9500-6C8809(config-test-signature-test)#show context
signature test
bssid 11-22-33-44-55-66
nx9500-6C8809(config-test-signature-test)#
```

#### Related Commands

`no` on page 1671 Disables a WIPS signature BSS ID

### dst-mac

Configures the destination MAC address to be used as match criteria

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

`dst-mac <MAC>`

#### Parameters

`dst-mac <MAC>`

`dst-mac <MAC>` Configures the destination MAC address of the packet examined for matching purposes and potential device exclusion

- `<MAC>` - Specify the destination MAC address.

#### Examples

```
nx9500-6C8809(config-test-signature-test)#dst-mac 55-66-77-88-99-00
nx9500-6C8809(config-test-signature-test)#show context
signature test
 bssid 11-22-33-44-55-66
 dst-mac 55-66-77-88-99-00
nx9500-6C8809(config-test-signature-test)#
```

#### Related Commands

`no` on page 1671 Disables a WIPS signature destination MAC address

### filter-ageout

Configures the filter-ageout duration in seconds. This is the duration a client, triggering a WIPS event, is excluded from RF Domain manager radio association.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
filter-ageout <1-86400>
```

#### Parameters

```
filter-ageout <1-86400>
```

|                         |                                                              |
|-------------------------|--------------------------------------------------------------|
| filter-ageout <1-86400> | Configures the filter-ageout duration from 1 - 86400 seconds |
|-------------------------|--------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config-test-signature-test)#filter-ageout 8
nx9500-6C8809(config-test-signature-test)#show context
signature test
 bssid 11-22-33-44-55-66
 dst-mac 55-66-77-88-99-00
 filter-ageout 8
nx9500-6C8809(config-test-signature-test)#
```

#### Related Commands

|                                 |                                               |
|---------------------------------|-----------------------------------------------|
| <a href="#">no</a> on page 1671 | Removes the configured filter-ageout duration |
|---------------------------------|-----------------------------------------------|

## frame-type

Configures the frame type used for matching with this WIPS policy signature

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
frame-type [all|assoc|auth|beacon|data|deauth|disassoc|mgmt|probe-req|probe-req|reassoc]
```

#### Parameters

```
frame-type [all|assoc|auth|beacon|data|deauth|disassoc|mgmt|probe-req|probe-req|reassoc]
reassoc]
```

|            |                                             |
|------------|---------------------------------------------|
| frame-type | Configures the frame type used for matching |
| all        | Matches all frame types                     |
| assoc      | Matches only association frames             |
| auth       | Matches only authentication frames          |
| beacon     | Matches only beacon frames                  |
| data       | Matches only data frames                    |

|            |                                       |
|------------|---------------------------------------|
| deauth     | Matches only de-authentication frames |
| disassoc   | Matches only disassociation frames    |
| mgmt       | Matches only management frames        |
| probe-req  | Matches only probe request frames     |
| probe-resp | Matches only probe response frames    |
| reassoc    | Matches only re-association frames    |

### Usage Guidelines

The frame type configured determines the SSID match type. To set the SSID match type as SSID, the frame type must be set to **beacon**, **probe-req** or **probe-resp**. For more information see, [ssid-match](#) on page 1668.

### Examples

```

nx9500-6C8809(config-test-signature-test)#frame-type reassoc
nx9500-6C8809(config-test-signature-test)#show context
signature test
 bssid 11-22-33-44-55-66
 dst-mac 55-66-77-88-99-00
 frame-type reassoc
 filter-ageout 8
nx9500-6C8809(config-test-signature-test)#

```

### Related Commands

|                                 |                                    |
|---------------------------------|------------------------------------|
| <a href="#">no</a> on page 1672 | Resets a WIPS signature frame type |
|---------------------------------|------------------------------------|

## interference-event

Configures this WIPS policy signature as Smart RF interference source

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
interference-event
```

### Parameters

None

### Examples

```

nx9500-6C8809(config-test-signature-test)#interference-event
nx9500-6C8809(config-test-signature-test)#show context
signature test
 interference-event
 bssid 11-22-33-44-55-66
 dst-mac 55-66-77-88-99-00
 frame-type reassoc
 filter-ageout 8
nx9500-6C8809(config-test-signature-test)#

```

### Related Commands

no on page 1672

Disables this WIPS policy signature as Smart RF interference source

mode

Enables this WIPS policy signature

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
mode enable
```

Parameters

```
mode enable
```

mode enable

Enables this WIPS signature

Examples

```
nx9500-6C8809(config-test-signature-test)#mode enable
nx9500-6C8809(config-test-signature-test)#
```

Related Commands

no on page 1672

Disables this WIPS signature

payload

Configures payload settings. The payload command sets a numerical index pattern and offset for this WIPS signature. Payload-based signatures detect patterns in the content of the file rather than attributes, such as a hash, allowing them to identify and block altered malware.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
payload <1-3> pattern <WORD> offset <0-255>
```

Parameters

```
payload <1-3> pattern <WORD> offset <0-255>
```

|                |                                                                                                                                                              |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| payload <1-3>  | Configures payload settings <ul style="list-style-type: none"><li>• &lt;1-3&gt; – Set the payload index from 1 - 3.</li></ul>                                |
| pattern <WORD> | Specifies the pattern to match: hex or string <ul style="list-style-type: none"><li>• &lt;WORD&gt; – Set the pattern name.</li></ul>                         |
| offset <0-255> | Specifies the payload offset to start the pattern match <ul style="list-style-type: none"><li>• &lt;0-255&gt; – Set the offset value from 0 - 255.</li></ul> |

## Examples

```
nx9500-6C8809(config-test-signature-test)#payload 1 pattern test offset 1
nx9500-6C8809(config-test-signature-test)#show context
signature test
 bssid 11-22-33-44-55-66
 dst-mac 55-66-77-88-99-00
 frame-type assoc
 filter-ageout 8
 payload 1 pattern test offset 1
nx9500-6C8809(config-test-signature-test)#
```

## Related Commands

|                                 |                                               |
|---------------------------------|-----------------------------------------------|
| <a href="#">no</a> on page 1671 | Removes payload index and associated settings |
|---------------------------------|-----------------------------------------------|

## src-mac

Configures a source MAC address for a packet examined for matching

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
src-mac <MAC>
```

## Parameters

```
src-mac <MAC>
```

|               |                                                                                                                                            |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| src-mac <MAC> | Configures the source MAC address to match <ul style="list-style-type: none"><li>• &lt;MAC&gt; – Specify the source MAC address.</li></ul> |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-test-signature-test)#src-mac 00-1E-E5-EA-1D-60
nx9500-6C8809(config-test-signature-test)#show context
signature test
 bssid 11-22-33-44-55-66
 src-mac 00-1E-E5-EA-1D-60
 dst-mac 55-66-77-88-99-00
 frame-type assoc
 filter-ageout 8
 payload 1 pattern test offset 1
nx9500-6C8809(config-test-signature-test)#
```

## Related Commands

|                                 |                                             |
|---------------------------------|---------------------------------------------|
| <a href="#">no</a> on page 1671 | Removes a WIPS signature source MAC address |
|---------------------------------|---------------------------------------------|

## ssid-match

Configures the SSID (and its character length) used as a match criteria

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533



- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
ssid-match [ssid|ssid-len]
ssid-match [ssid <SSID>|ssid-len <0-32>]
```

#### Parameters

```
ssid-match [ssid <SSID>|ssid-len <0-32>]
```

|                 |                                                                                                                                                                                                      |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ssid <SSID>     | Specifies the SSID match string <ul style="list-style-type: none"> <li>• &lt;SSID&gt; – Specify the SSID string.</li> </ul> <p><b>Note:</b> Specify the correct SSID to ensure proper filtering.</p> |
| ssid-len <0-32> | Specifies the length of the SSID <ul style="list-style-type: none"> <li>• &lt;0-32&gt; – Specify the SSID length from 0 - 32 characters.</li> </ul>                                                  |

#### Examples

```
nx9500-6C8809(config-test-signature-test)#ssid-match ssid PrinterLan
nx9500-6C8809(config-test-signature-test)#show context
signature test
 bssid 11-22-33-44-55-66
 src-mac 00-1E-E5-EA-1D-60
 dst-mac 55-66-77-88-99-00
 frame-type beacon
 ssid-match ssid PrinterLan
 filter-ageout 8
 payload 1 pattern test offset 1
nx9500-6C8809(config-test-signature-test)#
```

#### Related Commands

|                 |                             |
|-----------------|-----------------------------|
| no on page 1671 | Removes the configured SSID |
|-----------------|-----------------------------|

#### threshold-client

Configures the client threshold limit. This is the threshold limit per client that, when exceeded, signals the event.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
threshold-client <1-65535>
```

#### Parameters

```
threshold-client <1-65535>
```

|                            |                                                                                                                                                                            |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| threshold-client <1-65535> | Configures the client threshold limit <ul style="list-style-type: none"> <li>• &lt;1-65535&gt; – Set the threshold limit for a 60 second window from 1 - 65535.</li> </ul> |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-test-signature-test)#threshold-client 88
nx9500-6C8809(config-test-signature-test)#show context
signature test
 bssid 11-22-33-44-55-66
 src-mac 00-1E-E5-EA-1D-60
 dst-mac 55-66-77-88-99-00
 frame-type beacon
 ssid-match ssid PrinterLan
 filter-ageout 8
 threshold-client 88
 payload 1 pattern test offset 1
nx9500-6C8809(config-test-signature-test)#
```

## Related Commands

|                              |                                                                            |
|------------------------------|----------------------------------------------------------------------------|
| <code>no</code> on page 1671 | Removes the client threshold limit configured with a WIPS policy signature |
|------------------------------|----------------------------------------------------------------------------|

## threshold-radio

Configures the radio's threshold limit. When the radio exceeds the specified limit, an event is triggered.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
threshold-radio <1-65535>
```

## Parameters

```
threshold-radio <1-65535>
```

|                              |                                                                                                                                                                               |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| threshold-radio<br><1-65535> | Configures the radio's threshold limit <ul style="list-style-type: none"><li>• &lt;1-65535&gt; - Specify the threshold limit for a 60 second window from 1 - 65535.</li></ul> |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-test-signature-test)#threshold-radio 88
nx9500-6C8809(config-test-signature-test)#show context
signature test
 bssid 11-22-33-44-55-66
 src-mac 00-1E-E5-EA-1D-60
 dst-mac 55-66-77-88-99-00
 frame-type beacon
 ssid-match ssid PrinterLan
 filter-ageout 8
 threshold-client 88
 threshold-radio 88
 payload 1 pattern test offset 1
nx9500-6C8809(config-test-signature-test)#
```

## Related Commands

|                              |                                                                             |
|------------------------------|-----------------------------------------------------------------------------|
| <code>no</code> on page 1671 | Removes the radio's threshold limit configured with a WIPS policy signature |
|------------------------------|-----------------------------------------------------------------------------|

no

Negates a command or resets settings to their default. When used in the config WIPS policy signature mode, the no command resets or removes WIPS signature settings.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
no [bssid|dst-mac|filter-ageout|frame-type|interference-event|mode|payload|
src-mac|ssid-match|threshold-client|threshold-radio]
no [bssid|dst-mac|filter-ageout|frame-type|interference-event|mode enable|
payload <1-3>|src-mac|ssid-match [ssid|ssid-len]|threshold-client|threshold-radio]
```

#### Parameters

```
no <PARAMETERS>
```

|                 |                                                       |
|-----------------|-------------------------------------------------------|
| no <PARAMETERS> | Negates a command or resets settings to their default |
|-----------------|-------------------------------------------------------|

#### Usage Guidelines

The **no** command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

#### Examples

The following is the WIPS signature 'test' settings before the execution of the 'no' command:

```
nx9500-6C8809(config-test-signature-test)#show context
signature test
 bssid 11-22-33-44-55-66
 src-mac 00-1E-E5-EA-1D-60
 dst-mac 55-66-77-88-99-00
 frame-type beacon
 ssid-match ssid PrinterLan
 filter-ageout 8
 threshold-client 88
 threshold-radio 88
 payload 1 pattern test offset 1
nx9500-6C8809(config-test-signature-test)#
nx9500-6C8809(config-test-signature-test)#no mode enable
nx9500-6C8809(config-test-signature-test)#no bssid
nx9500-6C8809(config-test-signature-test)#no dst-mac
nx9500-6C8809(config-test-signature-test)#no src-mac
nx9500-6C8809(config-test-signature-test)#no filter-ageout
nx9500-6C8809(config-test-signature-test)#no threshold-client
nx9500-6C8809(config-test-signature-test)#no threshold-radio
```

The following is the WIPS signature 'test' settings after the execution of the 'no' command:

```
nx9500-6C8809(config-test-signature-test)#
signature test
 no mode enable
 frame-type beacon
 payload 1 pattern test offset 1
nx9500-6C8809(config-test-signature-test)
```

no

Negates a command or resets configured settings to their default. When used in the config WIPS policy mode, the no command negates or resets filters and thresholds.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
no [ap-detection|enable|event|history-throttle-duration|interference-event|signature|use]
no [enable|history-throttle-duration]
no ap-detection {ageout <{LINE-SINK}>}/air-termination/interferer-threshold <-100--10>/recurring-event-interval <0-10000>wait-time <{LINE-SINK}>}
no event [ap-anomaly|client-anomaly|enable-all-events|excessive]
no event ap-anomaly [ad-hoc-violation|airjack|ap-ssid-broadcast-in-beacon|asleep|impersonation-attack|null-porbe-response|transmitting-device-using-invalid-mac|unencrypted-wired-leakage|wireless-bridge]
no event client-anomaly [dos-broadcast-deauth|fuzzing-all-zero-macs|fuzzing-invalid-frame-type|fuzzing-invalid-mgmt-frames|fuzzing-invalid-seq-num|identical-src-and-dest-addr|invalid-8021x-frames|netstumbler-generic|non-conforming-data|wellenreiter] {filter-ageout <0-86400>}
no event excessive [80211-replay-check-failure|aggressive-scanning|auth-server-failures|decryption-failures|dos-assoc-or-auth-flood|dos-eapol-start-storm|dos-unicast-deauth-or-disassoc|eap-flood|eap-nak-flood|frames-from-unassoc-station] {filter-ageout <0-86400>}/threshold-client <0-65535>/threshold-radio <0-65535>}
no interference-event [non-conforming-data|wireless-bridge]
no signature <WIPS-SIGNATURE>
no use device-categorization
```

### Parameters

```
no <PARAMETERS>
```

no <PARAMETERS> Negates a command or resets configured settings to their default. When used in the config WIPS policy mode, the no command negates or resets filters and thresholds.

### Usage Guidelines

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

### Examples

The following example shows the WIPS Policy 'test' settings before the 'no' commands are executed:

```
nx9500-6C8809(config-wips-policy-test)#show context
wips-policy test
 history-throttle-duration 77
 event excessive 80211-replay-check-failure threshold-client 10 threshold-radio 99 filter-ageout 9
 event client-anomaly wellenreiter filter-ageout 99
 interference-event non-conforming-data
 ap-detection-ageout 50
```

```

ap-detection-wait-time 15
nx9500-6C8809(config-wips-policy-test)#
nx9500-6C8809(config-wips-policy-test)#no event client-anomaly wellenreiter filter-ageout
99
nx9500-6C8809(config-wips-policy-test)#no interference-event non-conforming-data
nx9500-6C8809(config-wips-policy-test)#no history-throttle-duration

```

The following example shows the WIPS Policy 'test' settings after the 'no' commands are executed:

```

nx9500-6C8809(config-wips-policy-test)#show context
wips-policy test
 event excessive 80211-replay-check-failure threshold-client 10 threshold-radio 99 filter-
ageout 9
 no event client-anomaly wellenreiter filter-ageout 99
 ap-detection-ageout 50
 ap-detection-wait-time 15
nx9500-6C8809(config-wips-policy-test)#

```

## use

Enables device categorization on this WIPS policy. This command uses an existing device categorization list. The list categorizes devices as authorized or unauthorized.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
use device-categorization <DEVICE-CATEGORIZATION>
```

### Parameters

```
use device-categorization <DEVICE-CATEGORIZATION>
```

|                                                  |                                                                                                                                                                                                               |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| device-categorization<br><DEVICE-CATEGORIZATION> | Associates a device categorization list <ul style="list-style-type: none"> <li>• &lt;DEVICE-CATEGORIZATION&gt; - Specify the device categorization object name to associate with this WIPS policy.</li> </ul> |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```

nx9500-6C8809(config-wips-policy-test)#use device-categorization test
nx9500-6C8809(config-wips-policy-test)#show context
wips-policy test
 event excessive 80211-replay-check-failure threshold-client 10 threshold-radio 99 filter-
ageout 9
 no event client-anomaly wellenreiter filter-ageout 99
 signature test
 interference-event
 bssid 11-22-33-44-55-66
 dst-mac 55-66-77-88-99-00
 frame-type reassoc
 filter-ageout 8
 threshold-client 88
 payload 1 pattern test offset 1
 ap-detection-ageout 50
 ap-detection-wait-time 15

```

---

```
use device-categorization test
nx9500-6C8809(config-wips-policy-test)#
```

### Related Commands

|                      |                                                                       |
|----------------------|-----------------------------------------------------------------------|
| <pre>no on</pre>     | Disables the use of a device categorization policy with a WIPS policy |
| <pre>page 1672</pre> |                                                                       |

# WLAN QoS Policy

## WLAN-QOS-POLICY

---

This chapter summarizes the WLAN QoS policy in the CLI command structure.

A WLAN QoS policy increases network efficiency by prioritizing data traffic. Prioritization reduces congestion. This is essential because of the lack of bandwidth for all users and applications. QoS helps ensure each WLAN on the wireless controller receives a fair share of the overall bandwidth, either equally or as per the proportion configured. Packets directed towards clients are classified into categories such as Video, Voice and Data. Packets within each category are processed based on the weights defined for each WLAN

Each WLAN QoS policy has a set of parameters which it groups into categories, such as management, voice and data. Packets within each category are processed based on the weights defined for each WLAN.

Use the (config) instance to configure WLAN QoS policy commands. To navigate to the WLAN QoS policy instance, use the following commands:

```
<DEVICE> (config)#wlan-qos-policy <POLICY-NAME>
nx9500-6C8809(config)#wlan-qos-policy test
nx9500-6C8809(config-wlan-qos-test)#?
WLAN QoS Mode commands:
 accelerated-multicast Configure accelerated multicast streams address and
 forwarding QoS classification
 classification Select how traffic on this WLAN must be classified
 (relative prioritization on the radio)
 multicast-mask Egress multicast mask (frames that match bypass the
 PSPqueue. This permits intercom mode operation
 without delay even in the presence of PSP clients)
 no Negate a command or set its defaults
 qos Quality of service
 rate-limit Configure traffic rate-limiting parameters on a
 per-wlan/per-client basis
 svp-prioritization Enable spectralink voice protocol support on this wlan
 voice-prioritization Prioritize voice client over other client (for
 non-WMM clients)
 wmm Configure 802.11e/Wireless MultiMedia parameters

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal
nx9500-6C8809(config-wlan-qos-test)#
```

## WLAN-QoS-Policy commands

WLAN QoS configurations differ significantly from QoS policies configured for radios. WLAN QoS configurations are designed to support the data requirements of wireless clients, including the data types they support and their network permissions. Radio QoS policies are specific to the transmit and receive characteristics of the connected radio's themselves, independent from the wireless clients these Access Point radios support.

The following table summarizes WLAN QoS policy configuration commands.

**Table 53: WLAN-QoS-Policy-Config Commands**

| Command                            | Description                                                                        |
|------------------------------------|------------------------------------------------------------------------------------|
| <code>accelerated-multicast</code> | Configures accelerated multicast stream addresses and forwards QoS classifications |
| <code>classification</code>        | Classifies WLAN traffic based on priority                                          |
| <code>multicast-mask</code>        | Configures the egress prioritization multicast mask                                |
| <code>no</code>                    | Negates a command or sets its default                                              |
| <code>qos</code>                   | Defines the QoS configuration                                                      |
| <code>rate-limit</code>            | Configures the WLAN traffic rate limit using a WLAN QoS policy                     |
| <code>svp-prioritization</code>    | Enables Spectralink voice protocol support on a WLAN                               |
| <code>voice-prioritization</code>  | Prioritizes voice client over other clients                                        |
| <code>wmm</code>                   | Configures 802.11e/wireless multimedia parameters                                  |



### Note

For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see [COMMON COMMANDS](#) on page 640.



### Note

The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore ( \_ ) character. In other words, the name of a device cannot contain an underscore.

## accelerated-multicast

Configures the accelerated multicast stream address and forwarding QoS classification

*Supported in the following platforms:*

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000



## Syntax

```
accelerated-multicast [<IP>|autodetect]
accelerated-multicast [<IP>|autodetect] {classification [background|best-effort|
trust|video|voice]}
```

## Parameters

```
accelerated-multicast [<IP>|autodetect] {classification [background|best-effort|
trust|video|voice]}
```

|                       |                                                                                                                                                                                                                                                                       |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| accelerated-multicast | Configures the accelerated multicast stream address and forwarding QoS classification                                                                                                                                                                                 |
| <IP>                  | Configures a multicast IP address in the A.B.C.D format. The system can configure up to 32 IP addresses for each WLAN QoS policy                                                                                                                                      |
| autodetect            | Allows the system to automatically detect multicast streams. This parameter allows the system to convert multicast streams to unicast, or to specify multicast streams converted to unicast.                                                                          |
| classification        | Optional. Configures the forwarding of the QoS classification (traffic class). When the stream is converted and queued for transmission, specify the type of classification applied to the stream. The options are: background, best-effort, trust, voice, and video. |
| background            | Forwards streams with background (low) priority. This parameter is common to both <IP> and autodetect.                                                                                                                                                                |
| best-effort           | Forwards streams with best effort (normal) priority. This parameter is common to both <IP> and autodetect.                                                                                                                                                            |
| trust                 | No change to the streams forwarding traffic class. This parameter is common to both <IP> and autodetect.                                                                                                                                                              |
| video                 | Forwards streams with video traffic priority. This parameter is common to both <IP> and autodetect.                                                                                                                                                                   |
| voice                 | Forwards streams with voice traffic priority. This parameter is common to both <IP> and autodetect.                                                                                                                                                                   |

## Examples

```
nx9500-6C8809(config-wlan-qos-test)#accelerated-multicast autodetect
classification voice
nx9500-6C8809(config-wlan-qos-test)#show context
wlan-qos-policy test
qos trust dscp
qos trust wmm
accelerated-multicast autodetect classification voice
nx9500-6C8809(config-wlan-qos-test)#
```

## classification

Specifies how traffic on this WLAN is classified. This classification is based on relative prioritization on the radio.

*Supported in the following platforms:*

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000

- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
classification [low|non-unicast|non-wmm|normal|video|voice|wmm]
classification [low|normal|video|voice|wmm]
classification non-unicast [voice|video|normal|low|default]
classification non-wmm [voice|video|normal|low]
```

### Parameters

```
classification [low|normal|video|voice|wmm]
```

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| low    | Optimized for background traffic. Implies all traffic on this WLAN is low priority on the radio                                                                                                                                                                                                                                                                                                                                      |
| normal | Optimized for best effort traffic. Implies all traffic on this WLAN is prioritized as best effort traffic on the radio                                                                                                                                                                                                                                                                                                               |
| video  | Optimized for video traffic. Implies all traffic on this WLAN is prioritized as video traffic on the radio                                                                                                                                                                                                                                                                                                                           |
| voice  | Optimized for voice traffic. Implies all traffic on this WLAN is prioritized as voice traffic on the radio                                                                                                                                                                                                                                                                                                                           |
| wmm    | Uses WMM based classification, using DSCP or 802.1p tags, to classify traffic into different queues. Implies WiFi Multimedia QoS extensions are enabled on this radio. This allows different traffic streams between the wireless client and the Access Point to be prioritized according to the type of traffic (voice, video etc). The WMM classification supports high throughput data rates required for 802.11n device support. |

```
classification non-unicast [voice|video|normal|low|default]
```

|             |                                                                                                                                                        |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| non-unicast | Optimized for non-unicast traffic. Implies all traffic on this WLAN is designed for broadcast or multiple destinations                                 |
| video       | Optimized for non-unicast video traffic. Implies all WLAN non-unicast traffic is classified and treated as video packets                               |
| voice       | Optimized for non-unicast voice traffic. Implies all WLAN non-unicast traffic is classified and treated as voice packets                               |
| normal      | Optimized for non-unicast best effort traffic. Implies all WLAN non-unicast traffic is classified and treated as normal priority packets (best effort) |
| low         | Optimized for non-unicast background traffic. Implies all WLAN non-unicast traffic is classified and treated as low priority packets (background)      |
| default     | Uses the default classification mode (same as unicast classification if WMM is disabled, normal if unicast classification is WMM)                      |

```
classification non-wmm [voice|video|normal|low]
```

|         |                                                                                                                                                       |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| non-wmm | Specifies how traffic from non-WMM clients is classified                                                                                              |
| voice   | Optimized for non-WMM voice traffic. Implies all WLAN non-WMM client traffic is classified and treated as voice packets                               |
| video   | Optimized for non-WMM video traffic. Implies all WLAN non-WMM client traffic is classified and treated as video packets                               |
| normal  | Optimized for non-WMM best effort traffic. Implies all WLAN non-WMM client traffic is classified and treated as normal priority packets (best effort) |
| low     | Optimized for non-WMM background traffic. Implies all WLAN non-WMM client traffic is classified and treated as low priority packets (background)      |

## Examples

```
nx9500-6C8809(config-wlan-qos-test)#classification wmm
nx9500-6C8809(config-wlan-qos-test)#classification non-wmm video
nx9500-6C8809(config-wlan-qos-test)#classification non-unicast normal
nx9500-6C8809(config-wlan-qos-test)#show context
wlan-qos-policy test
 classification non-wmm video
 classification non-unicast normal
 qos trust dscp
 qos trust wmm
 accelerated-multicast autodetect classification voice
nx9500-6C8809(config-wlan-qos-test)#
```

## multicast-mask

Configures an egress prioritization multicast mask for this WLAN QoS policy

Normally all multicast and broadcast packets are buffered until the periodic DTIM interval (indicated in the 802.11 beacon frame), when clients in power save mode wake to check for frames. However, for certain applications and traffic types, the administrator may want the frames transmitted immediately, without waiting for the DTIM interval. By configuring a primary or secondary prioritization multicast mask, the network administrator can indicate which packets are transmitted immediately.

*Supported in the following platforms:*

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
multicast-mask [primary|secondary] <MAC/MASK>
```

## Parameters

```
multicast-mask [primary|secondary] <MAC/MASK>
```

|                      |                                                                                                                                                                                                                                                                                                                                           |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| primary <MAC/MASK>   | Configures the primary egress prioritization multicast mask <ul style="list-style-type: none"><li>• &lt;MAC/MASK&gt; - Sets the MAC address and the mask in the AA-BB-CC-DD-EE-FF/XX-XX-XX-XX-XX-XX format</li></ul> <p><b>Note:</b> Setting masks is optional and only needed if there are traffic types requiring special handling.</p> |
| secondary <MAC/MASK> | Configures the primary egress prioritization multicast mask <ul style="list-style-type: none"><li>• &lt;MAC/MASK&gt; - Sets the MAC address and the mask in the AA-BB-CC-DD-EE-FF / XX-XX-XX-XX-XX-XX format</li></ul>                                                                                                                    |

## Examples

```
nx9500-6C8809(config-wlan-qos-test)#multicast-mask primary
11-22-33-44-55-66/22-33-44-55-66-77
nx9500-6C8809(config-wlan-qos-test)#show context
wlan-qos-policy test
 classification non-wmm video
 multicast-mask primary 11-22-33-44-55-66/22-33-44-55-66-77
```

```

classification non-unicast normal
qos trust dscp
qos trust wmm
accelerated-multicast autodetect classification voice
nx9500-6c8809(config-wlan-qos-test)#

```

## no

Removes this WLAN QoS Policy settings or reverts them to default values

*Supported in the following platforms:*

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```

no [accelerated-multicast|classification|multicast-mask|qos|rate-limit|
svp-prioritization|voice-prioritization|wmm]
no [accelerated-multicast [<IP>|autodetect]|classification {non-unicast|non-wmm}|
multicast-mask [primary|secondary]|qos trust [dscp|wmm]|svp-prioritization|
voice-prioritization]
no rate-limit [client|wlan] [from-air|to-air] {max-burst-size|rate|red-threshold}
no rate-limit [client|wlan] [from-air|to-air] {max-burst-size|rate|
red-threshold [background|best-effort|video|voice]}
no wmm [background|best-effort|power-save|qbss-load-element|video|voice]
no wmm [power-save|qbss-load-element]
no wmm [backgorund|best-effort|video|voice] [aifsn|cw-max|cw-min|txop-limit]

```

### Parameters

```

no [accelerated-multicast [<IP>|autodetect]|classification {non-unicast|non-wmm}|
multicast-mask [primary|secondary]|qos trust [dscp|wmm]|svp-prioritization|
voice-prioritization]

```

|                                            |                                                                                                                                                                                                                                                                                            |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| no accelerated-multicast [<IP> autodetect] | <p>Disables accelerated multicast streams and forwarding QoS classification</p> <ul style="list-style-type: none"> <li>• &lt;IP&gt; - Removes specified IP address. Specify the IP address</li> <li>• autodetect - Disables multicast streams automatic detection</li> </ul>               |
| no classification [non-unicast  non-wmm]   | <p>Disables WLAN classification scheme</p> <ul style="list-style-type: none"> <li>• non-unicast - Optional. Removes multicast and broadcast packet classification</li> <li>• non-wmm - Optional. Removes non-WMM client traffic classification</li> </ul>                                  |
| no multicast-mask [primary secondary]      | <p>Disables the egress prioritization primary or secondary multicast mask</p> <ul style="list-style-type: none"> <li>• primary - Removes the first egress multicast mask</li> <li>• secondary - Removes the second egress multicast mask</li> </ul>                                        |
| no qos trust [disquiet]                    | <p>Disables the QoS service</p> <ul style="list-style-type: none"> <li>• trust - Ignores the trust QOS values of ingressing packets</li> <li>• dscp - Ignores the IP DSCP values of ingressing packets</li> <li>• wmm - Ignores the 802.11 WMM QoS values of ingressing packets</li> </ul> |

|                         |                                                                                |
|-------------------------|--------------------------------------------------------------------------------|
| no svp-prioritization   | Disables <i>Spectralink Voice Protocol</i> (SVP) support on a WLAN             |
| no voice-prioritization | Disables voice client priority over other clients (applies to non-WMM clients) |

```
no rate-limit [client|wlan] [from-air|to-air] {max-burst-size|rate|
red-threshold [background|best-effort|video|voice]}
```

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| no rate-limit<br>[client wlan] | Disables traffic rate limit parameters <ul style="list-style-type: none"> <li>Disables client traffic rate limits</li> <li>Disables WLAN traffic rate limits</li> </ul>                                                                                                                                                                                                                                                                     |
| [from-air to-air]              | The following are common to the client and WLAN parameters: <ul style="list-style-type: none"> <li>from-air – Removes client/WLAN traffic rate limits in the up link direction. This is traffic from the wireless client to the network</li> <li>to-air – Removes client/WLAN traffic rate limits in the down link direction. This is traffic from the network to the wireless client</li> </ul>                                            |
| max-burst-size                 | Optional. Disables the maximum burst size value                                                                                                                                                                                                                                                                                                                                                                                             |
| rate                           | Optional. Disables the traffic rates configured for a wireless client or WLAN                                                                                                                                                                                                                                                                                                                                                               |
| red-threshold                  | Optional. Disables random early detection threshold values configured for the traffic class <ul style="list-style-type: none"> <li>background – Disables the low priority traffic (background) threshold value</li> <li>best-effort – Disables the normal priority traffic (best effort) threshold value</li> <li>video – Disables the video traffic threshold value</li> <li>voice – Disables the voice traffic threshold value</li> </ul> |

```
no wmm [power-save|qbss-load-element]
```

|                   |                                                                                       |
|-------------------|---------------------------------------------------------------------------------------|
| no wmm            | Disables 802.11e/wireless multimedia parameters                                       |
| power-save        | Disables support for WMM-Powersave (U-APSD)                                           |
| qbss-load-element | Disables support for the QBSS load information element in beacons and probe responses |

```
no wmm [background|best-effort|video|voice] [aifsn|cw-max|cw-min|txop-limit]
```

|             |                                                 |
|-------------|-------------------------------------------------|
| no wmm      | Disables 802.11e/wireless multimedia parameters |
| background  | Disables background access category parameters  |
| best-effort | Disables best effort access category parameters |
| video       | Disables video access category parameters       |
| voice       | Disables voice access category parameters       |

### Examples

The following example shows the WLAN QoS Policy 'test' settings before the 'no' commands are executed:

```
nx9500-6C8809(config-wlan-qos-test)#show context
wlan-qos-policy test
classification non-wmm video
multicast-mask primary 11-22-33-44-55-66/22-33-44-55-66-77
classification non-unicast normal
qos trust dscp
qos trust wmm
```

```

accelerated-multicast autodetect classification voice
nx9500-6C8809(config-wlan-qos-test)#
nx9500-6C8809(config-wlan-qos-test)#no classification non-wmm
nx9500-6C8809(config-wlan-qos-test)#no multicast-mask primary
nx9500-6C8809(config-wlan-qos-test)#no qos trust dscp

```

The following example shows the WLAN QoS Policy 'test' settings after the 'no' commands are executed:

```

nx9500-6C8809(config-wlan-qos-test)#show context
wlan-qos-policy test
 classification non-unicast normal
 no qos trust dscp
 qos trust wmm
 accelerated-multicast autodetect classification voice
nx9500-6C8809(config-wlan-qos-test)#

```

## qos

Enables QoS on this WLAN

*Supported in the following platforms:*

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
qos trust [dscp|wmm]
```

### Parameters

```
qos trust [dscp|wmm]
```

|                  |                                                                                                                                                                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| trust [dscp wmm] | Trusts the QoS values of ingressing packets <ul style="list-style-type: none"> <li>• dscp - Trusts the IP DSCP values of ingressing packets</li> <li>• wmm - Trusts the 802.11 WMM QoS values of ingressing packets</li> </ul> |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```

nx9500-6C8809(config-wlan-qos-test)#qos trust wmm
nx9500-6C8809(config-wlan-qos-test)#qos trust dscp
nx9500-6C8809(config-wlan-qos-test)#show context
wlan-qos-policy test
 classification non-unicast normal
 qos trust dscp
 qos trust wmm
 accelerated-multicast autodetect classification voice
nx9500-6C8809(config-wlan-qos-test)#

```

## rate-limit

Configures the WLAN traffic rate limits using the WLAN QoS policy

Excessive traffic causes performance issues or brings down the network entirely. Excessive traffic can be caused by numerous sources including network loops, faulty devices or malicious software such as a

worm or virus that has infected one or more devices at the branch. Rate limiting limits the maximum rate sent to or received from the wireless network (and WLAN) per wireless client. It prevents any single user from overwhelming the wireless network. It can also provide differential service for service providers. The uplink and downlink rate limits are usually configured on a RADIUS server using vendor specific attributes. Rate limits are extracted from the RADIUS server's response. When such attributes are not present, settings defined on the controller (access point, wireless controller, or service platform) are applied. An administrator can set separate QoS rate limits for upstream (data transmitted from the managed network) and downstream (data transmitted to the managed network).

Before defining rate limit thresholds for WLAN upstream and downstream traffic, it is recommended that you define the normal number of ARP, broadcast, multicast and unknown unicast packets that typically transmit and receive from each supported WMM access category. If thresholds are defined too low, normal network traffic (required by end-user devices) are dropped resulting in intermittent outages and performance problems.

Connected wireless clients can also have QoS rate limit settings defined in both the upstream and downstream direction.

*Supported in the following platforms:*

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
rate-limit [client|wlan] [from-air|to-air]
{max-burst-size/rate/red-threshold}
rate-limit [client|wlan] [from-air|to-air] {max-burst-size <2-1024>/
rate <50-1000000>}
rate-limit [client|wlan] [from-air|to-air]
{red-threshold [background <0-100>/ best-effort <0-100>/video <0-100>/
voice <0-100>]}
```

### Parameters

```
rate-limit [client|wlan] [from-air|to-air] {max-burst-size <2-1024>/
rate <50-1000000>}
```

|            |                                                                         |
|------------|-------------------------------------------------------------------------|
| rate-limit | Configures traffic rate limit parameters                                |
| client     | Configures traffic rate limiting parameters on a per-client basis       |
| wlan       | Configures traffic rate limiting parameters on a per-WLAN basis         |
| from-air   | Configures traffic rate limiting from a wireless client to the network  |
| to-air     | Configures the traffic rate limit from the network to a wireless client |

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| max-burst-size<br><2-1024> | Optional. Sets the maximum burst size from 2 - 1024 kbytes. The chances of the upstream or downstream packet transmission getting congested for the WLAN's client destination are reduced for smaller burst sizes. The default is 320 kbytes.<br><b>Note:</b> Smaller the burst, lesser are the chances of upstream packet transmission resulting in congestion for the WLAN's client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should then add a 10% margin (minimally) to allow for traffic bursts at the site. |
| rate <50-1000000>          | Optional. Sets the traffic rate from 50 - 1000000 kbps. This limit is the threshold value for the maximum number of packets received or transmitted over the WLAN from all access categories. Any traffic that exceeds the specified rate is dropped and a log message is generated. The default is 5000 kbps.                                                                                                                                                                                                                                                                                                                                                                                              |

```
rate-limit [client|wlan] [from-air|to-air]
{red-threshold [background <0-100>| best-effort <0-100>|video <0-100>|
voice <0-100>]}
```

|                        |                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| rate-limit             | Configures traffic rate limit parameters                                                                                                                                                                                                                                                                                                                           |
| client                 | Configures traffic rate limiting parameters on a per-client basis                                                                                                                                                                                                                                                                                                  |
| wlan                   | Configures traffic rate limiting parameters on a per-WLAN basis                                                                                                                                                                                                                                                                                                    |
| from-air               | Configures traffic rate limiting from a wireless client to the network                                                                                                                                                                                                                                                                                             |
| to-air                 | Configures the traffic rate limit from the network to a wireless client                                                                                                                                                                                                                                                                                            |
| red-threshold          | Configures random early detection threshold values for a designated traffic class                                                                                                                                                                                                                                                                                  |
| background<br><0-100>  | The following is common to the 'from-air' and 'to-air' parameters:<br>Optional. Sets a percentage value for background traffic in the upstream or downstream direction. Background traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold is 50% for traffic in both directions.                                 |
| best-effort<br><0-100> | The following is common to the 'from-air' and 'to-air' parameters:<br>Optional. Sets a percentage value for best effort traffic in the upstream or downstream direction. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold is 50% for traffic in both directions.                               |
| video <0-100>          | The following is common to the 'from-air' and 'to-air' parameters:<br>Optional. Sets a percentage value for video traffic in the upstream or downstream direction. Video traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold is 25% fro traffic in both directions.                                           |
| voice <0-100>          | The following is common to the 'from-air' and 'to-air' parameters:<br>Optional. Sets a percentage value for voice traffic in the upstream or downstream direction. Voice traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold is 0% for traffic in both directions. 0% means no early random drops will occur. |

### Usage Guidelines

The following information should be taken into account when configuring rate limits:

- Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general downstream rate is known by the network administrator (using a time trend analysis).
- Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis).



- Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis).
- Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis).

### Examples

```

nx9500-6C8809(config-wlan-qos-test)#rate-limit wlan from-air max-burst-size 6
nx9500-6C8809(config-wlan-qos-test)#rate-limit wlan from-air rate 55
nx9500-6C8809(config-wlan-qos-test)#rate-limit wlan from-air red-threshold best-effort 10
nx9500-6C8809(config-wlan-qos-test)#rate-limit client from-air red-threshold background 3
nx9500-6C8809(config-wlan-qos-test)#show context
wlan-qos-policy test
 classification non-wmm video
 multicast-mask primary 11-22-33-44-55-66/22-33-44-55-66-77
 classification non-unicast normal
 rate-limit wlan from-air rate 55
 rate-limit wlan from-air max-burst-size 6
 rate-limit wlan from-air red-threshold best-effort 10
 rate-limit client from-air red-threshold background 3
 qos trust dscp
 qos trust wmm
 accelerated-multicast autodetect classification voice
nx9500-6C8809(config-wlan-qos-test)#

```

## svp-prioritization

Enables WLAN SVP support on this WLAN QoS policy. SVP support enables the identification and prioritization of traffic from Spectralink/Ploycomm phones. This gives priority to voice, with voice management packets supported only on certain legacy VOIP phones. If the wireless client classification is WMM, non-WMM devices recognized as voice devices have all their traffic transmitted at voice priority. Devices are classified as voice, when they emit SIP, SCCP, or H323 traffic. Thus, selecting this option has no effect on devices supporting WMM..

This feature is enabled by default.

*Supported in the following platforms:*

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
svp-prioritization
```

### Parameters

None

### Examples

```

nx9500-6C8809(config-wlan-qos-test)#svp-prioritization
nx9500-6C8809(config-wlan-qos-test)#show context
wlan-qos-policy test
 classification non-wmm video
 svp-prioritization

```

```

multicast-mask primary 11-22-33-44-55-66/22-33-44-55-66-77
classification non-unicast normal
rate-limit wlan from-air rate 55
rate-limit wlan from-air max-burst-size 6
rate-limit wlan from-air red-threshold best-effort 10
rate-limit client from-air red-threshold background 3
qos trust dscp
qos trust wmm
accelerated-multicast autodetect classification voice
nx9500-6C8809(config-wlan-qos-test)#

```

## voice-prioritization

Prioritizes voice clients over other clients (for non-WMM clients). This gives priority to voice and voice management packets and is supported only on certain legacy VOIP phones. This feature is enabled by default.

*Supported in the following platforms:*

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
voice-prioritization
```

### Parameters

None

### Examples

```

nx9500-6C8809(config-wlan-qos-test)#voice-prioritization
nx9500-6C8809(config-wlan-qos-test)#show context
wlan-qos-policy test
classification non-wmm video
svp-prioritization
voice-prioritization
multicast-mask primary 11-22-33-44-55-66/22-33-44-55-66-77
classification non-unicast normal
rate-limit wlan from-air rate 55
rate-limit wlan from-air max-burst-size 6
rate-limit wlan from-air red-threshold best-effort 10
rate-limit client from-air red-threshold background 3
qos trust dscp
qos trust wmm
accelerated-multicast autodetect classification voice
nx9500-6C8809(config-wlan-qos-test)#

```

## wmm

Configures 802.11e/Wireless Multimedia (WMM) parameters for this WLAN QoS policy

WMM makes it possible for both home networks and Enterprises to decide which data streams are most important and assign them a higher traffic priority.

---

WMM's prioritization capabilities are based on the four access categories (background, best-effort, video, and voice). Higher the *Access Category* (AC) higher is the transmission probability over the controller managed WLAN. ACs correspond to the 802.1d priorities, facilitating interoperability with QoS policy management mechanisms. WMM enabled controllers coexist with legacy devices (not WMM-enabled).

Packets not assigned to a specific access category are categorized as best effort by default. Applications assign each data packet to a given access category. Categorized packets are added to one of four independent transmit queues (one per access category). The client has an internal collision resolution mechanism to address collision among different queues, which selects the frames with the highest priority to transmit.

The same mechanism deals with external collision, to determine which client should be granted the *Opportunity to Transmit* (TXOP). The collision resolution algorithm responsible for traffic prioritization is probabilistic and depends on two timing parameters that vary for each access category. These parameters are:

- The minimum interframe space, or Arbitrary Inter-Frame Space Number (AIFSN)
- The contention window, sometimes referred to as the random back off wait

Both values are smaller for high-priority traffic. The value of the contention window varies through time. Initially the contention window is set to a value that depends on the AC. As frames with the highest AC tend to have the lowest back off values, they are more likely to get a TXOP.

After each collision the contention window is doubled until a maximum value (also dependent on the AC) is reached. After successful transmission, the contention window is reset to its initial, AC dependant value. The AC with the lowest back off value gets the TXOP.

*Supported in the following platforms:*

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### *Syntax*

```
wmm [background|best-effort|power-save|qbss-load-element|video|voice]
wmm [power-save|qbss-load-element]
wmm [background|best-effort|video|voice] [aifsn <2-15>|cw-max <0-15>|
cw-min <0-15>|txop-limit <0-65535>]
```

### *Parameters*

```
wmm [power-save|qbss-load-element]
```

|                   |                                                                                                                                                                                              |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wmm               | Configures 802.11e/wireless multimedia parameters                                                                                                                                            |
| power-save        | Enables support for the WMM-Powersave mechanism. This mechanism, also known as <i>Unscheduled Automatic Power Save Delivery</i> (U-APSD), is specifically designed for WMM voice devices.    |
| qbps-load-element | Enables support for the <i>QOS Basic Service Set</i> (QBSS) load information element in beacons and probe response packets advertised by access packets. This feature is enabled by default. |

```
wmm [background|best-effort|video|voice] [aifsn <2-15>|cw-max <0-15>|
cw-min <0-15>|txop-limit <0-65535>]
```

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wmm           | Configures 802.11e/wireless multimedia parameters. This parameter enables the configuration of four access categories. Applications assign each data packet to one of these four access categories and queues them for transmission.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| background    | Configures background access category parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| best-effort   | Configures best effort access category parameters. Packets not assigned to any particular access category are categorized by default as having best effort priority                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| video         | Configures video access category parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| voice         | Configures voice access category parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| aifsn <2-15>  | Configures <i>Arbitrary Inter-Frame Space Number</i> (AIFSN) from 2 - 15. AIFSN is the wait time between data frames. This parameter is common to background, best effort, video and voice.<br>The default for traffic voice categories is 2<br>The default for traffic video categories is 2<br>The default for traffic best effort (normal) categories is 3<br>The default for traffic background (low) categories is 7 <ul style="list-style-type: none"> <li>• &lt;2-15&gt; – Sets a value from 2 - 15</li> </ul>                                                                                                                                                                                                                               |
| cw-max <0-15> | Configures the maximum contention window. Wireless clients pick a number between 0 and the minimum contention window to wait before retransmission. Wireless clients then double their wait time on a collision, until it reaches the maximum contention window. This parameter is common to background, best effort, video and voice.<br>The default for traffic voice categories is 3<br>The default for traffic video categories is 4<br>The default for traffic best effort (normal) categories is 10<br>The default for traffic background (low) categories is 10 <ul style="list-style-type: none"> <li>• &lt;0-15&gt; – ECW: the contention window. The actual value used is <math>(2^{ECW} - 1)</math>. Set a value from 0 - 15.</li> </ul> |

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>cw-min &lt;0-15&gt;</p>        | <p>Configures the minimum contention window. Wireless clients pick a number between 0 and the min contention window to wait before retransmission. Wireless clients then double their wait time on a collision, until it reaches the maximum contention window. This parameter is common to background, best effort, video and voice.</p> <p>The default for traffic voice categories is 2<br/> The default for traffic video categories is 3<br/> The default for traffic best effort (normal) categories is 4<br/> The default for traffic background (low) categories is 4</p> <ul style="list-style-type: none"> <li>• &lt;0-15&gt; – ECW: the contention window. The actual value used is <math>(2^{ECW} - 1)</math>. Set a value from 0 - 15.</li> </ul> |
| <p>txop-limit &lt;0-65535&gt;</p> | <p>Configures the transmit-opportunity (the interval of time during which a particular client has the right to initiate transmissions). This parameter is common to background, best effort, video and voice.</p> <p>The default for traffic voice categories is 47<br/> The default for traffic video categories is 94<br/> The default for traffic best effort (normal) categories is 0<br/> The default for traffic background (low) categories is 0</p> <ul style="list-style-type: none"> <li>• &lt;0-65535&gt; – Set a value from 0 - 65535 to configure the transmit-opportunity in 32 microsecond units.</li> </ul>                                                                                                                                    |

### Examples

```

nx9500-6C8809(config-wlan-qos-test)#wmm video txop-limit 9
nx9500-6C8809(config-wlan-qos-test)#wmm voice cw-min 6
nx9500-6C8809(config-wlan-qos-test)#show context
wlan-qos-policy test
 classification non-wmm video
 svp-prioritization
 voice-prioritization
 wmm video txop-limit 9
 wmm voice cw-min 6
 multicast-mask primary 11-22-33-44-55-66/22-33-44-55-66-77
 classification non-unicast normal
 rate-limit wlan from-air rate 55
 rate-limit wlan from-air max-burst-size 6
 rate-limit wlan from-air red-threshold best-effort 10
 rate-limit client from-air red-threshold background 3
 qos trust dscp
 qos trust wmm
 accelerated-multicast autodetect classification voice
nx9500-6C8809(config-wlan-qos-test)#

```

# L2TPV3 Policy

## L2TPV3-POLICY

---

This chapter summarizes *Layer 2 Tunnel Protocol Version 3* (L2TPv3) policy commands in the CLI command structure.

The L2TPv3 policy defines control and encapsulation protocols for tunneling different types of layer 2 frames between two IP nodes. The L2TPv3 control protocol controls dynamic creation, maintenance, and tear down of L2TP sessions. The L2TPv3 encapsulation protocol is used to multiplex and demultiplex L2 data streams between two L2TP nodes across an IP network.

L2TPv3 is an IETF standard used for transporting different types of layer 2 frames in an IP network (and Access Point profile). L2TPv3 defines control and encapsulation protocols for tunneling layer 2 frames between two IP nodes. Use L2TPv3 to create tunnels for transporting layer 2 frames. L2TPv3 enables WING supported controllers and Access Points to create tunnels for transporting Ethernet frames to and from bridge VLANs and physical ports. L2TPv3 tunnels can be defined between WING devices and other vendor devices supporting the L2TPv3 protocol.

Multiple pseudowires can be created within an L2TPv3 tunnel. WING supported devices support an Ethernet VLAN pseudowire type exclusively. A pseudowire is an emulation of a layer 2 point-to-point connection over a packet-switching network (PSN). A pseudowire was developed out of the necessity to encapsulate and tunnel layer 2 protocols across a layer 3 network. Ethernet VLAN pseudowires transport Ethernet frames to and from a specified VLAN. One or more L2TPv3 tunnels can be defined between tunnel end points. Each tunnel can have one or more L2TPv3 sessions. Each tunnel session corresponds to one pseudowire. An L2TPv3 control connection (an L2TPv3 tunnel) needs to be established between the tunneling entities before creating a session.



### Note

A pseudowire is an emulation of a layer 2 point-to-point connection over a *packet-switching network* (PSN). A pseudowire was developed out of the necessity to encapsulate and tunnel layer 2 protocols across a layer 3 network.

Ethernet VLAN pseudowires transport Ethernet frames to and from a specified VLAN. One or more L2TPv3 tunnels can be defined between tunnel end points. Each tunnel can have one or more L2TPv3 sessions. Each tunnel session corresponds to one pseudowire. An L2TPv3 control connection (a L2TPv3 tunnel) needs to be established between the tunneling entities before creating a session.

For optimal pseudowire operation, both the L2TPv3 session originator and responder need to know the pseudowire type and identifier. These two parameters are communicated during L2TPv3 session establishment. An L2TPv3 session created within an L2TPv3 connection also specifies multiplexing parameters for identifying a pseudowire type and ID.

The working status of a pseudowire is reflected by the state of the L2TPv3 session. If a L2TPv3 session is down, the pseudowire associated with it must be shut down. The L2TPv3 control connection keep-

alive mechanism can serve as a monitoring mechanism for the pseudowires associated with a control connection.



#### Note

If connecting an Ethernet port to another Ethernet port, the pseudowire type must be *Ethernet port*, if connecting an Ethernet VLAN to another Ethernet VLAN, the pseudowire type must be *Ethernet VLAN*.

This chapter is organized into the following sections:

- [l2tpv3-policy-commands](#)
- [l2tpv3-tunnel-commands](#)
- [l2tpv3-manual-session-commands](#)

## l2tpv3-policy-commands

Use the (config) instance to configure L2TPV3 policy parameters. To navigate to the L2TPV3 policy instance, use the following commands:

```
<DEVICE>(config)#l2tpv3 policy <L2TPV3-POLICY-NAME>
nx9500-6C8809(config)#l2tpv3 policy L2TPV3Policy1
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#?
L2tpv3 Policy Mode commands:
 cookie-size Size of the cookie field present in each l2tpv3 data
 message
 failover-delay Time interval for re-establishing the tunnel after
 the failover (RF-Domain
 manager/VRRP-master/Cluster-master failover)
 force-l2-path-recovery Enables force learning of servers, gateways etc.,
 behind the l2tpv3 tunnel when the tunnel is
 established
 hello-interval Configure the time interval (in seconds) between
 l2tpv3 Hello keep-alive messages exchanged in l2tpv3
 control connection
 no Negate a command or set its defaults
 reconnect-attempts Maximum number of attempts to reestablish the
 tunnel.
 reconnect-interval Time interval between the successive attempts to
 reestablish the l2tpv3 tunnel
 retry-attempts Configure the maximum number of retransmissions for
 signaling message
 retry-interval Time interval (in seconds) before the initiating a
 retransmission of any l2tpv3 signaling message
 rx-window-size Number of signaling messages that can be received
 without sending the acknowledgment
 tx-window-size Number of signaling messages that can be sent
 without receiving the acknowledgment

 clrscr Clears the display screen
 commit Commit all changes made in this session
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal
```

```
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#
```

The following table summarizes L2TPV3 policy configuration commands:

**Table 54: L2TPV3-Tunnel-Policy-Config Commands**

| Command                             | Description                                                                                                                |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <code>cookie-size</code>            | Configures the cookie field size for each L2TPV3 data packet                                                               |
| <code>failover-delay</code>         | Configures the L2TPV3 tunnel failover delay in seconds                                                                     |
| <code>force-12-path-recovery</code> | Enables the forced detection of servers and gateways behind the L2TPV3 tunnel                                              |
| <code>hello-interval</code>         | Configures the interval, in seconds, between L2TPV3 "Hello" keep-alive messages exchanged in the L2TPV3 control connection |
| <code>no</code>                     | Negates or reverts L2TPV3 tunnel commands                                                                                  |
| <code>reconnect-attempts</code>     | Configures the maximum number of retransmissions for signalling messages                                                   |
| <code>reconnect-interval</code>     | Configures the interval, in seconds, between successive attempts to re-establish a failed tunnel connection                |
| <code>retry-attempts</code>         | Configures the maximum number of retransmissions of signalling messages                                                    |
| <code>retry-interval</code>         | Configures the interval, in seconds, before initiating a retransmission of any L2TPV3 signaling message                    |
| <code>rx-window-size</code>         | Configures the number of signaling messages received without sending an acknowledgment                                     |
| <code>tx-window-size</code>         | Configures the number of signaling messages transmitted without receiving an acknowledgment                                |



**Note**

For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see [COMMON COMMANDS](#) on page 640.



**Note**

The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (\_) character. In other words, the name of a device cannot contain an underscore.

*cookie-size*

Configures the size of the cookie field present in each L2TPv3 data packet. L2TPv3 data packets contain a session cookie that identifies the session (pseudowire) corresponding to it. In a tunnel, the cookie is a 4-byte or 8-byte signature shared between the two tunnel endpoints. This signature is configured at both the source and destination routers. If the signature at both ends do not match, the data is dropped. All sessions within a tunnel have the same session cookie size.



### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
cookie-size [0|4|8]
```

### Parameters

```
cookie-size [0|4|8]
```

|                     |                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cookie-size [0 4 8] | Configures the cookie-field size for each data packet. Select one of the following options: <ul style="list-style-type: none"><li>• 0 - No cookie field present in each L2TPV3 data message (this is the default setting)</li><li>• 4 - 4 byte cookie field present in each L2TPV3 data message</li><li>• 8 - 8 byte cookie field present in each L2TPV3 data message</li></ul> |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#cookie-size 8
<exswl>(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
 cookie-size 8
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#
```

### Related Commands

|           |                                                                                                      |
|-----------|------------------------------------------------------------------------------------------------------|
| <b>no</b> | Resets the cookie-field size to its default (0 - no cookie field present in each L2TPV3 data packet) |
|-----------|------------------------------------------------------------------------------------------------------|

### *failover-delay*

Configures the L2TPV3 tunnel failover delay in seconds. This is the interval after which a failed over tunnel is re-established.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
fail-over <5-60>
```

### Parameters

```
fail-over <5-60>
```

|                  |                                                                                                                                                                                                                                                                   |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| fail-over <5-60> | Sets the delay interval to re-establish a failed L2TPV3 tunnel (RF-Domain manager/ VRRP-master/Cluster-master failover) <ul style="list-style-type: none"><li>• &lt;5-60&gt; - Specify a fail-over delay from 5 - 60 seconds. The default is 5 seconds.</li></ul> |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#failover-delay 30
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
hello-interval 200
failover-delay 30
retry-attempts 10
retry-interval 30
cookie-size 8
rx-window-size 9
tx-window-size 9
reconnect-interval 100
reconnect-attempts 8
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#
```

## Related Commands

|                                                                   |
|-------------------------------------------------------------------|
| <b>no</b> Resets the failover interval to its default (5 seconds) |
|-------------------------------------------------------------------|

### *force-l2-path-recovery*

Enables the forced detection of servers and gateways behind the L2TPV3 tunnel. This feature is disabled by default.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
force-l2-path-recovery
```

## Parameters

None

## Examples

```
<exsw1>(config-l2tpv3-policy-L2TPV3Policy1)#force-l2-path-recovery
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
hello-interval 200
failover-delay 30
retry-attempts 10
retry-interval 30
cookie-size 8
rx-window-size 9
tx-window-size 9
reconnect-interval 100
reconnect-attempts 8
force-l2-path-recovery
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#
```

## Related Commands

|                                                                                          |
|------------------------------------------------------------------------------------------|
| <b>no</b> Disables the forced detection of servers and gateways behind the L2TPV3 tunnel |
|------------------------------------------------------------------------------------------|

## *hello-interval*

Configures the interval, in seconds, between L2TPV3 "Hello" keep-alive messages exchanged in a L2TPV3 control connection.

### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### **Syntax**

```
hello-interval <1-3600>
```

### **Parameters**

```
hello-interval <1-3600>
```

|                            |                                                                                                                                |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| hello-interval<br><1-3600> | Configures the interval for L2TPV3 "Hello" keep-alive messages. Specify a value from 1 - 3600 seconds (default is 60 seconds). |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------|

### **Examples**

```
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#hello-interval 200
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
 hello-interval 200
 cookie-size 8
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#
```

### **Related Commands**

|           |                                                                             |
|-----------|-----------------------------------------------------------------------------|
| <b>no</b> | Resets the "Hello" keep-alive message interval to its default of 60 seconds |
|-----------|-----------------------------------------------------------------------------|

## *reconnect-attempts*

Configures the maximum number of attempts made to re-establish a tunnel connection

### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### **Syntax**

```
reconnect-attempts <0-8>
```

### **Parameters**

```
reconnect-attempts <0-8>
```

|                          |                                                                                                                                                    |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| reconnect-attempts <0-8> | Configures the maximum number of attempts made to re-establish a tunnel connection                                                                 |
|                          | <ul style="list-style-type: none"><li>• &lt;0-8&gt; - Specify a value from 0 - 8 (default is 0: configures infinite reconnect attempts).</li></ul> |

### Examples

```
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#reconnect-attempts 8
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
hello-interval 200
cookie-size 8
reconnect-attempts 8
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#
```

### Related Commands

|    |                                                                                                        |
|----|--------------------------------------------------------------------------------------------------------|
| no | Resets the maximum number of reconnect attempts to default (0: configures infinite reconnect attempts) |
|----|--------------------------------------------------------------------------------------------------------|

### *reconnect-interval*

Configures the interval, in seconds, between successive attempts to re-establish a failed tunnel connection

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
reconnect-interval <1-3600>
```

### Parameters

```
reconnect-interval <1-3600>
```

|                             |                                                                                                                                    |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| reconnect-interval <1-3600> | Configures the interval between successive attempts to re-establish a failed tunnel connection                                     |
|                             | <ul style="list-style-type: none"><li>• &lt;1-3600&gt; - Specify a value from 1 - 3600 seconds (default is 120 seconds).</li></ul> |

### Examples

```
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#reconnect-interval 100
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#
l2tpv3 policy L2TPV3Policy1
hello-interval 200
cookie-size 8
reconnect-interval 100
reconnect-attempts 8
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#
```

### Related Commands

|    |                                                                                                                     |
|----|---------------------------------------------------------------------------------------------------------------------|
| no | Resets the interval between successive attempts to re-establish a failed tunnel connection to default (120 seconds) |
|----|---------------------------------------------------------------------------------------------------------------------|

## *retry-attempts*

Configures the maximum number of attempts made to retransmit signalling messages. Use this command to specify how many retransmission cycles occur before determining the target tunnel peer is not reachable.

### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### **Syntax**

```
retry-attempts <1-10>
```

### **Parameters**

```
retry-attempts <1-10>
```

`retry-attempts <1-10>` Configures the maximum number of attempts made to retransmit signalling messages

- `<1-10>` - Specify a value from 1 - 10 (default is 5 attempts).

### **Examples**

```
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#retry-attempts 10
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
hello-interval 200
retry-attempts 10
cookie-size 8
reconnect-interval 100
reconnect-attempts 8
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#
```

### **Related Commands**

`no` Resets the maximum number of retransmissions for signalling messages to default (5 attempts)

## *retry-interval*

Configures the interval, in seconds, between two successive attempts at retransmitting a L2TPv3 signaling message

### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### **Syntax**

```
retry-interval <1-250>
```

## Parameters

retry-interval <1-250>

|                        |                                                                                                                                |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| retry-interval <1-250> | Configures the interval, in seconds, between two successive retransmission attempts                                            |
|                        | <ul style="list-style-type: none"><li>• &lt;1-250&gt; - Specify a value from 1 - 250 seconds (default is 5 seconds).</li></ul> |

## Examples

```
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#retry-interval 30
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
hello-interval 200
retry-attempts 10
retry-interval 30
cookie-size 8
reconnect-interval 100
reconnect-attempts 8
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#
```

## Related Commands

|    |                                                  |
|----|--------------------------------------------------|
| no | Resets the retry interval to default (5 seconds) |
|----|--------------------------------------------------|

### *rx-window-size*

Configures the number of signaling packets received without sending an acknowledgment

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

rx-window-size <1-15>

## Parameters

rx-window-size <1-15>

|                       |                                                                                                                       |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------|
| rx-window-size <1-15> | Configures the number of packets received without sending an acknowledgment                                           |
|                       | <ul style="list-style-type: none"><li>• &lt;1-15&gt; - Specify a value from 1 - 15 (default is 10 packets).</li></ul> |

## Examples

```
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#rx-window-size 9
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
hello-interval 200
retry-attempts 10
retry-interval 30
cookie-size 8
rx-window-size 9
reconnect-interval 100
reconnect-attempts 8
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#
```

## Related Commands

`no` Resets the number of packets received without sending an acknowledgement to default (10 packets)

### *tx-window-size*

Configures the number of signaling packets transmitted without receiving an acknowledgment

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
tx-window-size <1-15>
```

#### Parameters

```
tx-window-size <1-15>
```

`tx-window-size <1-15>` Configures the number of packets transmitted without receiving an acknowledgment

- `<1-15>` – Specify a value from 1 - 15 (default is 10 packets).

#### Examples

```
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#tx-window-size 9
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
 hello-interval 200
 retry-attempts 10
 retry-interval 30
 cookie-size 8
 rx-window-size 9
 tx-window-size 9
 reconnect-interval 100
 reconnect-attempts 8
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#
```

## Related Commands

`no` Resets the number of packets transmitted without receiving an acknowledgment to default (10 packets)

### *no*

Negates or reverts L2TPV3 policy settings to default

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
no [cookie-size|failover-delay|force-l2-path-recovery|hello-interval|
reconnect-attempts|reconnect-interval|retry-attempts|retry-interval|rx-window-size|
tx-window-size]
```

## Parameters

```
no <PARAMETERS>
```

|                 |                                                      |
|-----------------|------------------------------------------------------|
| no <PARAMETERS> | Negates or reverts L2TPV3 policy settings to default |
|-----------------|------------------------------------------------------|

## Examples

The following example shows the l2tpv3 policy 'L2TPV3Policy1' settings before the 'no' commands are executed:

```
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
 hello-interval 200
 retry-attempts 10
 retry-interval 30
 cookie-size 8
 reconnect-interval 100
 reconnect-attempts 50
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#no hello-interval
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#no reconnect-attempts
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#no reconnect-interval
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#no retry-attempts
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#no retry-interval
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#no cookie-size
```

The following example shows the l2tpv3 policy 'L2TPV3Policy1' settings after the 'no' commands are executed:

```
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#
```

## l2tpv3-tunnel-commands

Use the (profile or device context) instance to configure a L2TPv3 tunnel. To navigate to the tunnel configuration mode, use the following command in the profile context:

```
<DEVICE>(config-profile-default-rfs4000)#l2tpv3 tunnel <TUNNEL-NAME>
nx9500-6C8809(config-profile-default-rfs4000)#l2tpv3 tunnel Tunnel1
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1)#
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1)#?
L2tpv3 Tunnel Mode commands:
 establishment-criteria Set tunnel establishment criteria
 fast-failover Configure fast failover for l2tpv3 tunnels
 hostname Tunnel specific local hostname
 local-ip-address Configure the IP address for tunnel. If not
 specified, tunnel source ip address would be chosen
 automatically based on the tunnel peer ip address
 mtu Configure the mtu size for the tunnel
 no Negate a command or set its defaults
 peer Configure the l2tpv3 tunnel peers. At least one peer
 must be specified
 preempt Preemption of secondary tunnel when primary comes
 back
 preemption Preemption of secondary tunnel
```



```

router-id Tunnel specific local router ID
session Create / modify the specified l2tpv3 session
use Set setting to use

clrscr Clears the display screen
commit Commit all changes made in this session
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

```

```
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1)#
```

The following table summarizes L2TPV3 tunnel configuration commands:

**Table 55: L2TPV3-Tunnel-Config Commands**

| Command                                 | Description                                                                                                                       |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <code>establishment-criteria</code>     | Configures L2TPV3 tunnel establishment criteria                                                                                   |
| <code>fast-failover</code> on page 1702 | Configures fast-failover support on the L2TPv3 tunnel                                                                             |
| <code>hostname</code>                   | Configures tunnel specific local hostname                                                                                         |
| <code>local-ip-address</code>           | Configures the tunnel's IP address                                                                                                |
| <code>mtu</code>                        | Configures the tunnel's <i>Maximum Transmission Unit</i> (MTU) size                                                               |
| <code>no</code>                         | Negates or reverts L2TPV3 tunnel commands                                                                                         |
| <code>peer</code>                       | Configures the tunnel's peers                                                                                                     |
| <code>preempt</code> on page 1708       | Enables preemption of secondary tunnel when primary tunnel comes back                                                             |
| <code>preemption</code> on page 1709    | Delays the preemption of secondary tunnel. Use this command to configure the time to wait before preempting the secondary tunnel. |
| <code>router-id</code>                  | Configures the tunnel's local router ID                                                                                           |
| <code>session</code>                    | Creates/modifies specified L2TPV3 session                                                                                         |
| <code>use</code>                        | Configures a tunnel to use a specified L2TPV3 tunnel policy                                                                       |

### *establishment-criteria*

Configures L2TPV3 tunnel establishment criteria

A L2TPV3 tunnel is established from the current device to the NOC Controller when the current device becomes the VRRP master, cluster master, or RF Domain Manager. Similarly, the L2TPV3 tunnel is closed when the current device switches to standby or backup mode.

#### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533

- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
establishment-criteria [always|cluster-master|rf-domain-manager|vrrp-master <1-255>]
```

### Parameters

```
establishment-criteria [always|cluster-master|rf-domain-manager|vrrp-master <1-255>]
```

|                     |                                                                                                                                                                                                                                                                                                                                                            |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| always              | Always establishes a L2TPv3 tunnel from the current device to the NOC controller. This is the default setting.<br>The 'always' option indicates the device need not be a cluster-master, rf-domain-manager, or vrrp-master to establish a tunnel.                                                                                                          |
| cluster-master      | Establishes a L2TPv3 tunnel from the current device to the NOC controller, only when the current device becomes the cluster master<br><br><b>Note:</b> The L2TPv3 tunnel is closed when the current device switches back the standby or backup mode.                                                                                                       |
| rf-domain-manager   | Establishes a L2TPv3 tunnel from the current device to the NOC controller, only when the current device becomes the RF Domain manager<br><br><b>Note:</b> The L2TPv3 tunnel is closed when the current device switches back the standby or backup mode.                                                                                                    |
| vrrp-master <1-255> | Establishes a L2TPv3 tunnel from the current device to the NOC controller, only when the current device becomes the VRRP master <ul style="list-style-type: none"> <li>• &lt;1-255&gt; – Specify the VRRP group number from 1 - 255.</li> </ul> <b>Note:</b> The L2TPv3 tunnel is closed when the current device switches back the standby or backup mode. |

### Examples

```
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnell)#establishment-criteria
cluster-master
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnell)#show context
l2tpv3 tunnel Tunnell
 establishment-criteria cluster-master
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnell)#
```

### Related Commands

|    |                            |
|----|----------------------------|
| no | Resets to default (always) |
|----|----------------------------|

### *fast-failover*

Configures fast-failover support on the L2TPv3 tunnel. When configured, devices, using this profile, send tunnel requests to both peers, and in turn, establish tunnels with both peers. If not configured, tunnel establishment occurs on one peer, with failover and other functionality the same as legacy behavior. In case fast failover is configured when an active tunnel, with one peer, already exists, the tunnel establishment process is re-initiated with both peers. Of the two tunnels established, one is marked active while the other is standby. The sessions and routes from the active tunnel are only pushed to the dataplane, resulting in creation of data sessions. However, if the active tunnel fails,

sessions and routes from the standby tunnel are pushed to the dataplane thereby providing almost immediate fail over. Both tunnels individually perform connection health checkups through hello intervals. This option is disabled by default.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
fast-failover {aggressive}
```

#### Parameters

```
fast-failover {aggressive}
```

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| fast-failover | Configures fast-failover support on the L2TPv3 tunnel                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| aggressive    | Optional. When enabled, tunnel initiation hello requests are set to zero. For failure detections, hello attempts are not retried, regardless of the number of retry attempts configured. This option is disabled by default.<br><br><b>Note:</b> The hello-interval and retry-attempts parameters are defined in the L2TPv3 Policy context. For more information on configuring an L2TPv3 policy, see <a href="#">l2tpv3-policy-commands</a> on page 1691. For more information on associating an L2TPv3 policy to an L2TPv3 tunnel, see <a href="#">use</a> on page 1712. |

#### Examples

```
nx9500-6C8809(config-profile testNX9500-l2tpv3-tunnel-TestTunnel2)#show context
include-factory | include fast-failover
 no fast-failover
nx9500-6C8809(config-profile testNX9500-l2tpv3-tunnel-TestTunnel2)#
nx9500-6C8809(config-profile testNX9500-l2tpv3-tunnel-TestTunnel2)#fast-failover
aggressive
nx9500-6C8809(config-profile testNX9500-l2tpv3-tunnel-TestTunnel2)#show context
l2tpv3 tunnel TestTunnel2
 fast-failover aggressive
nx9500-6C8809(config-profile testNX9500-l2tpv3-tunnel-TestTunnel2)#
```

#### Related Commands

|                                 |                                                    |
|---------------------------------|----------------------------------------------------|
| <a href="#">no</a> on page 1713 | Removes fast-failover support on the L2TPv3 tunnel |
|---------------------------------|----------------------------------------------------|

#### hostname

Configures the tunnel's local hostname

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

hostname <WORD>

## Parameters

hostname <WORD>

|                 |                                                                                                                                            |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| hostname <WORD> | Configures the tunnel's local hostname <ul style="list-style-type: none"><li>&lt;WORD&gt; - Specify the tunnel's local hostname.</li></ul> |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1)#hostname TunnelHost1
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1)#show context
 l2tpv3 tunnel Tunnel1
 hostname TunnelHost1
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1)#
```

## Related Commands

|    |                                     |
|----|-------------------------------------|
| no | Removes the tunnel's local hostname |
|----|-------------------------------------|

## *local-ip-address*

Configures the tunnel's source IP address. If no IP address is specified, the tunnel's source IP address is automatically configured based on the tunnel peer's IP address.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

local-ip-address <IP>

## Parameters

local-ip-address <IP>

|                       |                                                                                                                                                                                                                                                                                                             |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| local-ip-address <IP> | Configures the L2TPv3 tunnel's source IP address <ul style="list-style-type: none"><li>&lt;IP&gt; - Specify the tunnel's IP address. Ensure the IP address is available (or will become available - virtual IP) on an interface. Modifying a tunnel's local IP address re-establishes the tunnel.</li></ul> |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1)#local-ip-address
172.16.10.2
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1)#show context
 l2tpv3 tunnel Tunnel1
 local-ip-address 172.16.10.2
 hostname TunnelHost1
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1)#
```

## Related Commands

|                 |                                                                    |
|-----------------|--------------------------------------------------------------------|
| <code>no</code> | Resets the tunnel's local IP address and re-establishes the tunnel |
|-----------------|--------------------------------------------------------------------|

### *mtu*

Configures the MTU size for this tunnel. This value determines the packet size transmitted over this tunnel.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
mtu <128-1460>
```

#### Parameters

```
mtu <128-1460>
```

|                                   |                                                                                                                                                                             |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>mtu &lt;128-1460&gt;</code> | Configures the MTU size for this tunnel <ul style="list-style-type: none"><li>• &lt;128-1460&gt; - Specify a value from 128 - 1460 bytes (default is 1460 bytes).</li></ul> |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1)#mtu 1280
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1)#show context
l2tpv3 tunnel Tunnel1
 local-ip-address 172.16.10.2
 mtu 1280
 hostname TunnelHost1
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1)#
```

## Related Commands

|                 |                                                                     |
|-----------------|---------------------------------------------------------------------|
| <code>no</code> | Resets the MTU size for this manual session to default (1460 bytes) |
|-----------------|---------------------------------------------------------------------|

### *peer*

Configures the L2TPv3 tunnel's peers. At least one peer must be specified.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
peer <1-2> {hostname/ip-address/ipsec-secure/router-id/udp}
peer <1-2> {hostname [<HOSTNAME>/any]} {ipsec-secure/router-id/udp}
peer <1-2> {ip-address <IP>} {hostname/ipsec-secure/router-id/udp}
peer <1-2> {ipsec-secure} {gw [<IP>/<WORD>]}
peer <1-2> {router-id [<IP>/<WORD>/any]} {ipsec-secure/udp}
peer <1-2> {udp} {ipsec-secure/port <1-65535>}
```

## Parameters

```
peer <1-2> {hostname [<HOSTNAME>/any]} {ipsec-secure/router-id/udp}
```

|                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| peer <1-2>                                                | <p>Configures the tunnel's peer ID</p> <ul style="list-style-type: none"><li>• &lt;1-2&gt; - Specify the ID from 1 - 2. The peer ID identifies the primary (ID 1) secondary (ID 2) peers. The L2TPv3 tunnel is established with the primary peer. The secondary peer is used for tunnel failover. If the peer is not specified, tunnel establishment does not occur.</li></ul> <p><b>Note:</b> At any time the tunnel is established with only one peer, unless fast-failover support is configured on the L2TPv3 tunnel. For more information, see <a href="#">fast-failover</a> on page 1702.</p> |
| hostname<br>[<HOSTNAME>/any]                              | <p>Optional. Configures the peers' hostname. The hostname options are:</p> <ul style="list-style-type: none"><li>• &lt;HOSTNAME&gt; - Specifies the hostname as FQDN (Fully Qualified Domain Name) or partial DN or any other name</li><li>• any - Peer name is not specified. If the hostname is 'any' this tunnel is considered as responder only and will allow incoming connection from any host.</li></ul>                                                                                                                                                                                     |
| ipsec-secure {gw<br>[<IP>/<WORD>]}                        | <p>After specifying the peer hostname, optionally specify the IPSec settings:</p> <ul style="list-style-type: none"><li>• ipsec-secure - Optional. Enables auto IPSec on the L2TPv3 tunnel<ul style="list-style-type: none"><li>• gw - Optional. Configures the IPSec gateway. Use one of the following options to configure the IPSec gateway:<ul style="list-style-type: none"><li>&lt;IP&gt; - Configures IPSec gateway's IP address</li><li>&lt;WORD&gt; - Configures IPSec gateway's hostname</li></ul></li></ul></li></ul>                                                                    |
| router-id [<IP><br><WORD>/any]                            | <p>After specifying the peer hostname, optionally specify router ID settings:</p> <ul style="list-style-type: none"><li>• router-id - Optional. Configures the peer's router ID in one of the following formats:<ul style="list-style-type: none"><li>• &lt;IP&gt; - Peer router ID in the IP address (A.B.C.D) format</li><li>• &lt;WORD&gt; - Peer router ID range (for example, 100-120)</li><li>• any - Peer router ID is not specified. This allows incoming connection from any router ID.</li></ul></li></ul>                                                                                |
| udp {ipsec-secure<br>gw/port <1-65535><br>{ipsec-secure}} | <p>After specifying the peer hostname, optionally specify UDP settings:<br/>The UDP option configures the encapsulation mode for this tunnel.</p> <ul style="list-style-type: none"><li>• UDP - Optional. Configures UDP encapsulation (default encapsulation is IP)<ul style="list-style-type: none"><li>• ipsec-secure gw - Optional. Enables auto IPSec</li><li>• port &lt;1-65535&gt; {ipsec-secure} - Optional. Configures the peer's UDP port running the L2TPv3 service from 1 - 65535. After specifying the peer UDP port, optionally configure the IPSec settings.</li></ul></li></ul>     |

```
peer <1-2> {ip-address <IP>} {hostname/ipsec-secure/router-id/udp}
```

|                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| peer <1-2>                                                    | Configures the tunnel's peer ID from 1 - 2. At any time the tunnel is established with only one peer.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| ip-address <IP>                                               | Optional. Configures the peer's IP address in the A.B.C.D format <ul style="list-style-type: none"> <li>• &lt;IP&gt; - Specify the peer's IP address.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                           |
| hostname<br>[<FQDN> any]                                      | After specifying the peer IP address, optionally specify the peer's hostname:<br>Optional. Configures the peers' hostname. The hostname options are: <ul style="list-style-type: none"> <li>• &lt;FQDN&gt; - Specifies the hostname as FQDN or partial DN</li> <li>• any - Peer name is not specified. If the hostname is 'any' this tunnel is considered as responder only and will allow incoming connection from any host.</li> </ul>                                                                                                                   |
| ipsec-secure {gw<br>[<IP> <WORD>]}                            | After specifying the peer IP address, optionally specify the IPSec settings: <ul style="list-style-type: none"> <li>• ipsec-secure - Optional. Enables auto IPSec <ul style="list-style-type: none"> <li>• gw - Optional. Configures the IPSec gateway. Use one of the following options to configure the IPSec gateway: <ul style="list-style-type: none"> <li>&lt;IP&gt; - Configures IPSec gateway's IP address</li> <li>&lt;WORD&gt; - Configures IPSec gateway's hostname</li> </ul> </li> </ul> </li> </ul>                                          |
| router-id<br>[<A.B.C.D> <br><WORD>  any]                      | After specifying the peer IP address, optionally specify the router ID using one of the following options: <ul style="list-style-type: none"> <li>• router-id - Optional. Configures the peer's router-id in one of the following formats: <ul style="list-style-type: none"> <li>• &lt;A.B.C.D&gt; - Peer router ID in the IP address (A.B.C.D) format</li> <li>• &lt;WORD&gt; - Peer router ID range (for example, 100-120)</li> <li>• any - Peer router ID is not specified. This allows incoming connection from any router ID.</li> </ul> </li> </ul> |
| udp {ipsec-secure<br>gw port<br><1-65535> {ipsec-<br>secure}} | After specifying the peer IP address, optionally specify the peer's UDP port settings:<br>The UDP option configures the encapsulation mode for this tunnel. <ul style="list-style-type: none"> <li>• UDP - Optional. Configures UDP encapsulation (default encapsulation is IP)</li> <li>• ipsec-secure gw - Optional. Enables auto IPSec</li> <li>• port &lt;1-65535&gt; - Optional. Configures the peer's UDP port running the L2TPv3 service from 1 - 65535. After specifying the peer UDP port, optionally configure the IPSec settings.</li> </ul>    |

```
peer <1-2> {ipsec-secure} {gw [<IP>|<WORD>]}
```

|                                    |                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| peer <1-2>                         | Configures the tunnel's peer ID from 1 - 2. At any time the tunnel is established with only one peer.                                                                                                                                                                                                                                                                              |
| ipsec-secure {gw<br>[<IP> <WORD>]} | Optional. Enables auto IPSec for this peer <ul style="list-style-type: none"> <li>• gw - Optional. Configures the IPSec gateway. Use one of the following options to configure the IPSec gateway: <ul style="list-style-type: none"> <li>• &lt;IP&gt; - Configures IPSec gateway's IP address</li> <li>• &lt;WORD&gt; - Configures IPSec gateway's hostname</li> </ul> </li> </ul> |

```
peer <1-2> {router-id [<IP>|<WORD>|any]} {ipsec-secure|udp}
```

|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| peer <1-2>                                                 | Configures the tunnel peer ID from 1 - 2. At any time the tunnel is established with only one peer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| router-id<br>[<A.B.C.D> <br><WORD>  any]                   | Optional. Configures the peer's router-id in one of the following formats: <ul style="list-style-type: none"> <li>• &lt;A.B.C.D&gt; – Peer router ID in the IP address (A.B.C.D) format</li> <li>• &lt;WORD&gt; – Peer router ID range (for example, 100-120)</li> <li>• any – Peer router ID is not specified. This allows incoming connection from any router ID.</li> </ul>                                                                                                                                                                                                        |
| ipsec-secure {gw<br>[<IP> <WORD>]}                         | After specifying the peer's router ID, optionally specify the IPsec settings. <ul style="list-style-type: none"> <li>• ipsec-secure – Optional. Enables auto IPsec <ul style="list-style-type: none"> <li>• gw – Optional. Configures the IPsec gateway. Use one of the following options to configure the IPsec gateway: <ul style="list-style-type: none"> <li>&lt;IP&gt; – Configures IPsec gateway's IP address</li> <li>&lt;WORD&gt; – Configures IPsec gateway's hostname</li> </ul> </li> </ul> </li> </ul>                                                                    |
| udp {ipsec-secure<br>gw  port <1-65535><br>{ipsec-secure}} | After specifying the peer's router ID, optionally specify the IPsec settings. The UDP option configures the encapsulation mode for this tunnel. <ul style="list-style-type: none"> <li>• UDP – Optional. Configures UDP encapsulation (default encapsulation is IP) <ul style="list-style-type: none"> <li>• ipsec-secure gw – Optional. Enables auto IPsec</li> <li>• port &lt;1-65535&gt; – Optional. Configures the peer's UDP port running the L2TPv3 service from 1 - 65535. After specifying the peer UDP port, optionally configure the IPsec settings.</li> </ul> </li> </ul> |

```
peer <1-2> {udp} {ipsec-secure/port <1-65535>}
```

|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| peer <1-2>                                              | Configures the tunnel peer ID from 1 - 2. At any time the tunnel is established with only one peer.                                                                                                                                                                                                                                                                                                                        |
| udp {ipsec-secure <br>port <1-65535><br>{ipsec-secure}} | Optional. Configures UDP encapsulation for this tunnel's peer (default encapsulation is IP) <ul style="list-style-type: none"> <li>• ipsec-secure – Optional. Configures IPsec gateway on this peer UDP port</li> <li>• port &lt;1-65535&gt; – Optional. Configures the peer's UDP port running the L2TPv3 service from 1 - 65535. After specifying the peer UDP port, optionally configure the IPsec settings.</li> </ul> |

## Examples

```
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1)#peer 2 hostname
tunnel1peer1 udp port 100
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1)#show context
l2tpv3 tunnel Tunnel1
 peer 2 hostname tunnel1peer1 udp port 100
 establishment-criteria cluster-master
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1)#
```

## Related Commands

|    |                                             |
|----|---------------------------------------------|
| no | Removes the peer configured for this tunnel |
|----|---------------------------------------------|

*preempt*

Enables preemption of secondary tunnel when primary tunnel comes back



### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
preempt enable
```

### Parameters

```
preempt enable
```

|                |                                                                                                            |
|----------------|------------------------------------------------------------------------------------------------------------|
| preempt enable | Enables preemption of secondary tunnel when primary tunnel comes back. This option is disabled by default. |
|----------------|------------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config-profile test-l2tpv3-tunnel-tunnell)#preempt enable
nx9500-6C8809(config-profile test-l2tpv3-tunnel-tunnell)#show context
l2tpv3 tunnel tunnell
preempt enable
nx9500-6C8809(config-profile test-l2tpv3-tunnel-tunnell)#
```

### Related Commands

|                 |                                                                        |
|-----------------|------------------------------------------------------------------------|
| no on page 1713 | Disables preemption of secondary tunnel when primary tunnel comes back |
|-----------------|------------------------------------------------------------------------|

### *preemption*

Delays the preemption of secondary tunnel. Use this command to configure the time to wait before preempting the secondary tunnel.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
preemption delay <60-600>
```

### Parameters

```
preemption delay <60-600>
```

|                           |                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| preemption delay <60-600> | When the primary L2TPv3 tunnel goes down, the system waits and watches for the tunnel to come back, for a specified time, before preempting the secondary tunnel. Use this command to configure that time period. <ul style="list-style-type: none"><li>• delay &lt;60-600&gt; - Specify a value from 60 - 600 seconds. The default is 60 seconds.</li></ul> |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-profile test-l2tpv3-tunnel-tunnell)#preemption delay 100
nx9500-6C8809(config-profile test-l2tpv3-tunnel-tunnell)#show context
 l2tpv3 tunnel tunnell
 preempt enable
 preemption delay 100
nx9500-6C8809(config-profile test-l2tpv3-tunnel-tunnell)#
```

## Related Commands

|                              |                                                                  |
|------------------------------|------------------------------------------------------------------|
| <code>no</code> on page 1713 | Resets the secondary tunnel preemption wait time to default (60) |
|------------------------------|------------------------------------------------------------------|

## *router-id*

Configures the tunnel's local router ID

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
router-id [<1-4294967295>|<IP>]
```

## Parameters

```
router-id [<1-4294967295>|<IP>]
```

|                                                        |                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>router-id [&lt;1-4294967295&gt; &lt;IP&gt;]</pre> | Configures the tunnel's local router ID in one of the following formats: <ul style="list-style-type: none"><li>• &lt;1-4294967295&gt; - Router ID in the number format (from 1- 4294967295)</li><li>• &lt;IP&gt; - Router ID in IP address format (A.B.C.D)</li></ul> |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnell)#router-id 2000
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnell)#show context
 l2tpv3 tunnel Tunnell
 peer 2 hostname tunnellpeer1 udp port 100
 router-id 2000
 establishment-criteria cluster-master
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnell)#
```

## Related Commands

|                 |                                |
|-----------------|--------------------------------|
| <code>no</code> | Removes the tunnel's router ID |
|-----------------|--------------------------------|

## *session*

Configures a session's pseudowire ID, which describes the session's purpose. The session established message sends this pseudowire ID to the L2TPv3 peer.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
session <L2TPV3-SESSION-NAME> [pseudowire-id|rate-limit]
session <L2TPV3-SESSION-NAME> pseudowire-id <1-4294967295> traffic-source
vlan <VLAN-ID-RANGE> {native-vlan <1-4094>}
session <L2TPV3-SESSION-NAME> rate-limit [egress|ingress] rate <50-1000000>
max-burst-size <2-1024>
```

### Parameters

```
session <L2TPV3-SESSION-NAME> pseudowire-id <1-4294967295> traffic-source
vlan <VLAN-ID-RANGE> {native-vlan <1-4094>}
```

|                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| session <L2TPV3-SESSION-NAME>       | Configures this session's name <ul style="list-style-type: none"><li>• &lt;L2TPV3-SESSION-NAME&gt; - Specify the L2TPV3 session name (should not exceed 31 characters in length). A tunnel is usable only if it has one or more session(s) (having specific session names) configured. The L2TPv3 tunnel has no idle timeout, it closes when the last tunnel session is closed.</li></ul> |
| pseudowire-id <1-4294967295>        | Configures the pseudowire ID for this session from 1- 4204067295<br>A pseudowire is an emulation of a layer 2 point-to-point connection over a <i>packet-switching network</i> (PSN). A pseudowire is needed to encapsulate and tunnel layer 2 protocols across a layer 3 network.                                                                                                        |
| traffic-source vlan <VLAN-ID-RANGE> | Configures VLAN as the traffic source for this tunnel <ul style="list-style-type: none"><li>• &lt;VLAN-ID-RANGE&gt; - Configures VLAN range list of traffic source. Specify the VLAN IDs as a range (for example, 10-20, 25, 30-35).</li></ul>                                                                                                                                            |
| native-vlan <1-4094>                | Optional - Configures the native VLAN ID for this session, which is not tagged <ul style="list-style-type: none"><li>• &lt;1-4094&gt; - Specify the native VLAN ID from 1- 4094.</li></ul>                                                                                                                                                                                                |

```
session <L2TPV3-SESSION-NAME> rate-limit [egress|ingress] rate <50-1000000> max-burst-size
<2-1024>
```

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| session <L2TPV3-SESSION-NAME> | Configures this session's name <ul style="list-style-type: none"><li>• &lt;L2TPV3-SESSION-NAME&gt; - Specify the L2TPV3 session name (should not exceed 31 characters in length). A tunnel is usable only if it has one or more session(s) (having specific session names) configured. The L2TPv3 tunnel has no idle timeout, it closes when the last tunnel session is closed.</li></ul>                                                                                                                                                                                                                   |
| rate-limit [egress ingress]   | Configures a rate for incoming and/or outgoing traffic on this L2TPv3 tunnel. When configured, this option limits the rate at which data is sent to or received from L2TPv3 tunnel members. <ul style="list-style-type: none"><li>• egress - Applies the specified rate to outbound traffic, from the L2TPv3 tunnel (going out from access points, wireless controllers, and service platforms) to the network</li><li>• ingress - Applies the specified rate to inbound traffic, from the network to the L2TPV3 tunnel (coming in to access points, wireless controllers, and service platforms)</li></ul> |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| rate <50-1000000>       | Specify the data rate, in kilobits per second, for the incoming and/or outgoing traffic <ul style="list-style-type: none"> <li>&lt;50-1000000&gt; – Specify a value from 50 - 1000000 kbps. The default is 5000 Kbps.</li> </ul>                                                                                                                                                                                                                           |
| max-burst-size <2-1024> | Configures the maximum burst size, in kilobytes, for incoming/outgoing traffic rate limiting (depending on the direction selected) on a L2TPv3 tunnel. <ul style="list-style-type: none"> <li>&lt;2-1024&gt; – Specify the maximum burst size from 2 - 1024 kbytes. Smaller the burst size, lesser are the chances of the upstream packet transmission resulting in congestion of the L2TPv3 tunnel traffic. The default setting is 320 kbytes.</li> </ul> |

### Usage Guidelines

The working status of a pseudowire is reflected by the state of the L2TPv3 session. If the corresponding session is L2TPv3 down, the pseudowire associated with it must be shut down.

### Examples

```

nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1)#session
tunnel1peer1session1 pseudowire-id 5000 traffic-source vlan 10-20 native-vlan 1
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1)#show context
l2tpv3 tunnel Tunnel1
 peer 2 hostname tunnel1peer1 udp port 100
 session tunnel1peer1session1 pseudowire-id 5000 traffic-source vlan 10-20 native-vlan 1
 router-id 2000
 establishment-criteria cluster-master
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1)#

```

### Related Commands

|    |                   |
|----|-------------------|
| no | Removes a session |
|----|-------------------|

*use*

Configures a tunnel to use a specified L2TPV3 tunnel policy and specified critical resources

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```

use [critical-resource|l2tpv3-policy]
use critical-resource <CRM-NAME1> {<CRM-NAME2>} {<CRM-NAME3>} {<CRM-NAME4>}
use l2tpv3-policy <L2TPV3-POLICY-NAME>

```

### Parameters

```

use critical-resource <CRM-NAME1> {<CRM-NAME2>} {<CRM-NAME3>} {<CRM-NAME4>}

```

use critical-resource <CRM-NAME1> {<CRM-NAME2>} {<CRM-NAME3>} {<CRM-NAME4>}

Specifies the critical resource(s) to use with this tunnel

- <CRM1-NAME> - Specify the first critical resource name (should be existing).
- <CRM-NAME2/3/4> - Optional. Specify the second/third/fourth critical resource names. Maximum of four critical resources can be monitored.

**Note:** In case of tunnel initiator, L2TPv3 tunnel is established only if the critical resources identified by the <CRM-NAME1>..... <CRM-NAME4> arguments are available at the time of tunnel establishment.

**Note:** In case of L2TPv3 tunnel termination, all incoming tunnel establishment requests are rejected if the critical resources specified by the <CRM-NAME1>..... <CRM-NAME4> arguments are not available.

use l2tpv3-policy <L2TPV3-POLICY-NAME>

use l2tpv3-policy <L2TPV3-POLICY-NAME>

Associates a specified L2TPV3 policy with this tunnel

- <L2TPV3-POLICY-NAME> - Specify the policy name.

## Examples

```
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1)#use l2tpv3-policy L2TPV3Policy1
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1)#show context
l2tpv3 tunnel Tunnel1
 peer 2 hostname tunnellopeer1 udp port 100
 use l2tpv3-policy L2TPV3Policy1
 session tunnellopeer1session1 pseudowire-id 5000 traffic-source vlan 10-20 native-vlan 1
 router-id 2000
 establishment-criteria cluster-master
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1)#
```

## Related Commands

**no** Removes the L2TPV3 policy configured with a tunnel and reverts to the default tunnel policy

*no*

Negates or reverts a L2TPv3 tunnel settings to default

## Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
no [establishment-criteria|fast-failover|hostname|local-ip-address|mtu|peer <1-2>|preempt enable|preemption delay|router-id|session|use]
```

## Parameters

no <PARAMETERS>

no <PARAMETERS>

Negates or reverts a L2TPv3 tunnel settings to default

## Examples

The tunnel settings before the 'no' command is executed:

```
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1)#show context
l2tpv3 tunnel Tunnel1
 local-ip-address 172.16.10.2
 mtu 1280
 hostname TunnelHost1
 establishment-criteria cluster-master
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1)#
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1)#no local-ip
-address
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1)#no mtu
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1)#no hostname
```

The tunnel settings after the 'no' command is executed:

```
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1)#show context
l2tpv3 tunnel Tunnel1
 establishment-criteria cluster-master
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1)#
```

## l2tpv3-manual-session-commands

After a successful tunnel connection and establishment, individual sessions can be created. Each session is a single data stream. After successful session establishment, data corresponding to that session (pseudowire) can be transferred. If a session is down, the pseudowire associated with it is shut down as well.

Use the (profile-context) instance to manually configure a L2TPv3 manual session. To navigate to the L2TPv3 manual session configuration mode, use the following command in the profile context:

```
<DEVICE>(config-profile-default-rfs4000)#l2tpv3 manual-session <SESSION-NAME>
nx9500-6C8809(config-profile-default-rfs4000)#l2tpv3 manual-session test
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#?
L2tpv3 Manual Session Mode commands:
 local-cookie The local cookie for the session
 local-ip-address Configure the IP address for tunnel. If not specified,
 tunnel source ip address would be chosen automatically
 based on the tunnel peer ip address
 local-session-id Local session id for the session
 mtu Configure the mtu size for the tunnel
 no Negate a command or set its defaults
 peer Configure L2TPv3 manual session peer
 remote-cookie The remote cookie for the session
 remote-session-id Remote session id for the session
 traffic-source Traffic that is tunneled

 clrscr Clears the display screen
 commit Commit all changes made in this session
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#
```

The following table summarizes L2TPV3 manual session configuration commands:

**Table 56: L2TPV3-Manual-Session-Config Commands**

| Command                        | Description                                                  |
|--------------------------------|--------------------------------------------------------------|
| <code>local-cookie</code>      | Configures the manual session's local cookie field size      |
| <code>local-ip-address</code>  | Configures the manual session's local source IP address      |
| <code>local-session-id</code>  | Configures the manual session's local session ID             |
| <code>mtu</code>               | Configures the MTU size for the manual session tunnel        |
| <code>no</code>                | Negates or reverts L2TPV3 manual session commands to default |
| <code>peer</code>              | Configures the manual session's peers                        |
| <code>remote-cookie</code>     | Configures the remote cookie for the manual session          |
| <code>remote-session-id</code> | Configures the manual session's remote session ID            |
| <code>traffic-source</code>    | Configures the traffic source tunneled by the manual session |

### *local-cookie*

Configures the local cookie field size for the manual session

#### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### **Syntax**

```
local-cookie size [4|8] <1-4294967295> {<1-4294967295>}
```

#### **Parameters**

```
local-cookie size [4|8] <1-4294967295> {<1-4294967295>}
```

|                                      |                                                                                                                                                                                                             |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>local-cookie size [4 8]</code> | Configures the local cookie field size for this manual session. The options are: <ul style="list-style-type: none"> <li>• 4 - 4 byte local cookie field</li> <li>• 8 - 8 byte local cookie field</li> </ul> |
| <code>&lt;1-4294967295&gt;</code>    | Configures the local cookie value first word. Applies to both the 4 byte and 8 byte local cookies                                                                                                           |
| <code>&lt;1-4294967295&gt;</code>    | Optional - Configures the local cookie value second word. Applicable to only 8 byte cookies. This parameter is ignored for 4 byte cookies.                                                                  |

#### **Examples**

```
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#local-cookie size
8 200 300
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#show context
l2tpv3 manual-session test
 local-cookie size 8 200 300
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#
```

## Related Commands

**no** Removes the local cookie size configured for a manual session

### *local-ip-address*

Configures the manual session's source IP address. If no IP address is specified, the tunnel's source IP address is automatically configured based on the tunnel peer IP address. This parameter is applicable when establishing the session and responding to incoming requests.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
local-ip-address <IP>
```

#### Parameters

```
local-ip-address <IP>
```

|                       |                                                                                                                                                        |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| local-ip-address <IP> | Configures the manual session's source IP <ul style="list-style-type: none"><li>• &lt;IP&gt; – Specify the IP address in the A.B.C.D format.</li></ul> |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#local-ip-address 1.2.3.4
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#show context
l2tpv3 manual-session test
local-cookie size 8 200 300
local-ip-address 1.2.3.4
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#
```

## Related Commands

**no** Resets the manual session's local source IP address. This re-establishes the session.

### *local-session-id*

Configures the manual session's local session ID

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
local-session-id <1-63>
```



## Parameters

local-session-id <1-63>

|                         |                                                                                                                                                                                                                       |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| local-session-id <1-63> | Configures this manual session's local session ID                                                                                                                                                                     |
|                         | <ul style="list-style-type: none"><li>&lt;1-63&gt; - Specify the ID from 1 - 63. This is the pseudowire ID for the session. This pseudowire ID is sent in a session establishment message to the L2TP peer.</li></ul> |

## Examples

```
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#local-session-id 1
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#show context
l2tpv3 manual-session test
 local-cookie size 8 200 300
 local-ip-address 1.2.3.4
 local-session-id 1
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#
```

## Related Commands

|    |                                               |
|----|-----------------------------------------------|
| no | Removes the manual session's local session ID |
|----|-----------------------------------------------|

## mtu

Configures the MTU size for the manual session tunnel. The MTU is the size (in bytes) of the largest protocol data unit the layer can pass between tunnel peers in this session. A larger MTU means processing fewer packets for the same amount of data.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

mtu <128-1460>

## Parameters

mtu <128-1460>

|                |                                                                                                                                   |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------|
| mtu <128-1460> | Configures the MTU size for this manual session tunnel                                                                            |
|                | <ul style="list-style-type: none"><li>&lt;128-1460&gt; - Specify a value from 128 - 1460 bytes (default is 1460 bytes).</li></ul> |

## Examples

```
nx9500-6C8809(config-profile default-rfs7000-l2tpv3-manual-session-test)#mtu 200
nx9500-6C8809(config-profile default-rfs7000-l2tpv3-manual-session-test)#show context
l2tpv3 manual-session test
 local-cookie size 8 200 300
 local-ip-address 1.2.3.4
 mtu 200
 local-session-id 1
nx9500-6C8809(config-profile default-rfs7000-l2tpv3-manual-session-test)#
```

## Related Commands

**no** Resets the MTU size for this manual session to default (1460 bytes)

### *peer*

Configures peer(s) allowed to establish the manual session tunnel. The peers are identified by their IP addresses.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
peer ip-address <IP> {udp {port <1-65535>}}
```

#### Parameters

```
peer ip-address <IP> {udp {port <1-65535>}}
```

|                                         |                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>peer ip-address &lt;IP&gt;</code> | Configures the tunnel's peer IP address in the A.B.C.D format                                                                                                                                                                                                                                                                     |
| <code>udp {port &lt;1-65535&gt;}</code> | Optional. Configures the UDP encapsulation mode for this tunnel (default encapsulation is IP) <ul style="list-style-type: none"><li>• <code>port &lt;1-65535&gt;</code> - Optional. Configures the peer's UDP port running the L2TPv3 service.</li><li>• <code>&lt;1-65535&gt;</code> - Specify a value from 1 - 65535.</li></ul> |

#### Examples

```
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#peer ip-address 5.6.7.8 udp port 150
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#show context
l2tpv3 manual-session test
 local-cookie size 8 200 300
 local-ip-address 1.2.3.4
 peer ip-address 5.6.7.8 udp port 150
 mtu 200
 local-session-id 1
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#
```

## Related Commands

**no** Removes the manual session's peer configuration

### *remote-cookie*

Configures the manual session's remote cookie field size

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
remote-cookie size [4|8] <1-4294967295> {<1-4294967295>}
```

### Parameters

```
remote-cookie size [4|8] <1-4294967295> {<1-4294967295>}
```

|                          |                                                                                                                                                                                                             |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| remote-cookie size [4 8] | Configures the remote cookie field size for this manual session. The options are: <ul style="list-style-type: none"><li>• 4 – 4 byte remote cookie field</li><li>• 8 – 8 byte remote cookie field</li></ul> |
| <1-4294967295>           | Configures the remote cookie value first word. Applies to both the 4 byte and 8 byte local cookies                                                                                                          |
| <1-4294967295>           | Optional – Configures the remote cookie value second word. Applicable to only 8 byte cookies. This parameter is ignored for 4 byte cookies.                                                                 |

### Examples

```
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#remote-cookie
size 8 400 700
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#show context
l2tpv3 manual-session test
 local-ip-address 1.2.3.4
 peer ip-address 5.6.7.8 udp port 150
 mtu 200
 local-session-id 1
 remote-cookie size 8 400 700
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#
```

### Related Commands

|    |                                                       |
|----|-------------------------------------------------------|
| no | Removes the manual session's remote cookie field size |
|----|-------------------------------------------------------|

### *remote-session-id*

Configures the manual session's remote ID. This ID is passed in the establishment of the tunnel session.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
remote-session-id <1-4294967295>
```

## Parameters

```
remote-session-id <1-4294967295>
```

|                                     |                                                                                                                                                        |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| remote-session-id<br><1-4294967295> | Configures this manual session's remote ID <ul style="list-style-type: none"><li>&lt;1-4294967295&gt; - Specify a value from 1 - 4294967295.</li></ul> |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#remote-session-id 200
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#show context
l2tpv3 manual-session test
 local-ip-address 1.2.3.4
 peer ip-address 5.6.7.8 udp port 150
 local-session-id 1
 remote-session-id 200
 remote-cookie size 8 400 700
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#
```

## Related Commands

|    |                                        |
|----|----------------------------------------|
| no | Removes the manual session's remote ID |
|----|----------------------------------------|

### *traffic-source*

Configures the traffic source tunneled by this session

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
traffic-source vlan <VLAN-ID-RANGE> {native-vlan <1-4094>}
```

## Parameters

```
traffic-source vlan <VLAN-ID-RANGE> {native-vlan <1-4094>}
```

|                                        |                                                                                                                                                                                                                                             |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| traffic-source vlan<br><VLAN-ID-RANGE> | Configures VLAN as the traffic source for this tunnel <ul style="list-style-type: none"><li>&lt;VLAN-ID-RANGE&gt; - Configures VLAN range list of traffic source. Specify the VLAN IDs as a range (for example, 10-20, 25, 30-35)</li></ul> |
| native-vlan <1-4094>                   | Optional - Configures the native VLAN ID for this session, which is not tagged <ul style="list-style-type: none"><li>&lt;1-4094&gt; - Specify the native VLAN ID from 1- 4094.</li></ul>                                                    |

## Examples

```
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#traffic-source vlan 50-60 native-vlan 2
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#show context
l2tpv3 manual-session test
 local-ip-address 1.2.3.4
 peer ip-address 5.6.7.8 udp port 150
```

```
traffic-source vlan 50-60 native-vlan 2
local-session-id 1
remote-session-id 200
remote-cookie size 8 400 700
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#
```

## Related Commands

|                                                                      |
|----------------------------------------------------------------------|
| <b>no</b> Removes the traffic source configured for a manual session |
|----------------------------------------------------------------------|

*no*

Negates or reverts L2TPV3 manual session settings to default

## Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
no [local-cookie|local-ip-address|local-session-id|mtu|peer|remote-cookie|
remote-session-id|traffic-source]
```

## Parameters

```
no <PARAMETERS>
```

|                                                                                           |
|-------------------------------------------------------------------------------------------|
| <b>no &lt;PARAMETERS&gt;</b> Negates or reverts L2TPv3 manual session settings to default |
|-------------------------------------------------------------------------------------------|

## Examples

The following example shows the manual session 'test' settings before the 'no' commands are executed:

```
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#show context
l2tpv3 manual-session test
 local-ip-address 1.2.3.4
 peer ip-address 5.6.7.8 udp port 150
 traffic-source vlan 50-60 native-vlan 2
 local-session-id 1
 remote-session-id 200
 remote-cookie size 8 400 700
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#no local-ip-
address
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#no local-session-
id
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#no remote-session-
id
```

The following example shows the manual session 'test' settings after the 'no' commands are executed:

```
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#show context
l2tpv3 manual-session test
 peer ip-address 5.6.7.8 udp port 150
 traffic-source vlan 50-60 native-vlan 2
 remote-cookie size 8 400 700
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-manual-session-test)#
```

## Router Mode

### ROUTER-MODE

---

This chapter summarizes OSPF (Open Shortest Path First) router mode commands in the CLI command structure. All router-mode commands are available on both device and profile modes.

OSPF is an IGMP (interior gateway protocol) used within large autonomous systems to distribute routing information. OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer, which makes routing decisions based solely on the destination IP address found in IP packets.

OSPF detects changes in the topology, like a link failure, and plots a new loop-free routing structure. It computes the shortest path for each route using a shortest path first algorithm. Link state data is maintained on each router and is periodically updated on all OSPF member routers. This enables routers to synchronize routing tables.

OSPF uses a route table managed by the link cost (external metrics) defined for each routing interface. The cost could be the distance of a router (round-trip time), link throughput or link availability.

Use the (config) instance to configure router commands. To navigate to the (config-router-mode) instance, use the following command:

```
<DEVICE>(config-profile-<PROFILE-NAME>)#router ospf
nx9500-6C8809(config-profile-default-rfs4000)#router ospf
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#?
Router OSPF Mode commands:
 area OSPF area
 auto-cost OSPF auto-cost
 default-information Distribution of default information
 ip Internet Protocol (IP)
 network OSPF network
 no Negate a command or set its defaults
 ospf OSPF
 passive Make OSPF Interface as passive
 redistribute Route types redistributed by OSPF
 route-limit Limit for number of routes handled OSPF process
 router-id Router ID

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-profile default-rfs4000-router-ospf)#
```

## router-mode-commands

The following table summarizes OSPF router configuration mode commands:

**Table 57: OSPF-Router Config Mode Commands**

| Command                          | Description                                                       |
|----------------------------------|-------------------------------------------------------------------|
| <code>area</code>                | Specifies OSPF enabled interfaces                                 |
| <code>auto-cost</code>           | Specifies the reference bandwidth in terms of Mbits per second    |
| <code>default-information</code> | Controls the distribution of default information                  |
| <code>ip</code>                  | Configures <i>Internet Protocol</i> (IP) default gateway priority |
| <code>network</code>             | Defines OSPF network settings                                     |
| <code>ospf</code>                | Enables OSPF                                                      |
| <code>passive</code>             | Specifies the configured OSPF interface as passive interface      |
| <code>redistribute</code>        | Specifies the route types redistributed by OSPF                   |
| <code>route-limit</code>         | Specifies the limit for the number of routes managed by OSPF      |
| <code>router-id</code>           | Specifies the router ID for OSPF                                  |
| <code>no</code>                  | Negates a command or sets its defaults                            |



### Note

For information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see [COMMON COMMANDS](#) on page 640.



### Note

The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore ( `_` ) character. In other words, the name of a device cannot contain an underscore.

## `area`

Configures OSPF network areas (OSPF enables interfaces)

An OSPF network can be subdivided into routing areas to simplify administration and optimize traffic utilization. Areas are logical groupings of hosts and networks, including routers having interfaces connected to an included network. Each area maintains a separate link state database whose information may be summarized towards the rest of the network by the connecting router. Areas are identified by 32-bit IDs, expressed either in decimal, or octet-based dot-decimal notation. Areas can be defined as: stub area, totally-stub, non-stub, nssa, totally nssa. Each of these area types have been discussed further in the [area-type](#) on page 1725 section of this chapter.

At least one default area, bearing number '0', should be configured for every OSPF network. In case of multiple areas, the default area 0 forms the backbone of the network. The default area 0 is used as a link to the other areas. Each area has its own link-state database.

A router running OSPF sends hello packets to discover neighbors and elect a designated router. The hello packet includes link state information and list of neighbors. OSPF is savvy with layer 2 topologies.

If on a point-to-point link, OSPF knows it is sufficient, and the link stays up. If on a broadcast link, the router waits for election before determining if the link is functional.

### Supported in the following platforms:

- Access Points — AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX

### Syntax

```
area [<0-4294967295>|<IP>]
```

### Parameters

```
area [<0-4294967295>|<IP>]
```

|                |                                                                                                                                                                      |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| area           | Defines an OSPF area                                                                                                                                                 |
| <0-4294967295> | Defines an OSPF area in the form of a 32 bit integer <ul style="list-style-type: none"><li>• &lt;0-4294967295&gt; - Specify the value from 0 - 4294967295.</li></ul> |
| <IP>           | Defines an OSPF area in the form of an IP address <ul style="list-style-type: none"><li>• &lt;IP&gt; - Specify the IP address.</li></ul>                             |

### Examples

```
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#area 4
nx9500-6C8809(config-profile default-rfs4000-router-ospf-area-0.0.0.4)#?
Router OSPF Area Mode commands:
 area-type OSPF area type
 authentication Authentication scheme for OSPF area
 no Negate a command or set its defaults
 range Routes matching this range are considered for summarization
 (ABR only)

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-profile default-rfs4000-router-ospf-area-0.0.0.4)#
nx9500-6C8809(config-profile default-rfs4000-router-ospf-area-0.0.0.4)#show context
 area 0.0.0.4
nx9500-6C8809(config-profile default-rfs4000-router-ospf-area-0.0.0.4)#
```

### Related Commands

The following table summarizes the OSPF area configuration mode commands:



**Table 58: OSPF-Area-Mode Commands**

| Command                                           | Description                                                  |
|---------------------------------------------------|--------------------------------------------------------------|
| <code>area-type</code>                            | Configures a particular OSPF area as STUB or NSSA            |
| <code>authentication</code>                       | Specifies the authentication scheme used for the OSPF area   |
| <code>range</code>                                | Specifies the routes matching address/mask for summarization |
| <code>no</code> (area-config-mode 'no' command)   | Negates a command or sets its defaults                       |
| <code>no</code> (router-config-mode 'no' command) | Removes area configuration settings                          |

### area-type

Configures a particular OSPF area as STUB, Totally STUB, NSSA or Totally NSSA

Areas can be defined as:

- `stub` area - Is an area that does not receive route advertisements external to the *autonomous system* (AS), and routing from within the area is based entirely on a default route.
- `totally-stub` - Is an area that does not allow summary routes and external routes. A default route is the only way to route traffic outside of the area. When there is only one route out of the area, fewer routing decisions are needed, lowering system resource utilization.
- `non-stub` - Is an area that imports autonomous system external routes and forwards to other areas. However, it still cannot receive external routes from other areas.
- `nssa` - A NSSA (Not-So-Stubby Area) is an extension of a stub that allows the injection of limited external routes into a stub area. If selecting NSSA, no external routes, except a default route, enter the area.
- `totally nssa` - Is a NSSA using 3 and 4 summary routes are not flooded into this type of area. It is also possible to declare an area both totally stubby and not-so-stubby, which means that the area will receive only the default route from area 0.0.0.0, but can also contain an ASBR (Autonomous System Boundary Router) that accepts external routing information and injects it into the local area, and from the local area into area 0.0.0.0.

Supported in the following platforms:

- Access Points — AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX

### Syntax

```

area-type [nssa|stub]
area-type nssa {default-cost|no-summary|translate-always|translate-candidate|
translate-never}
area-type nssa {default-cost <0-16777215> {no-summary}|no-summary
{default-cost <0-16777215>}}
area-type nssa {translate-always|translate-candidate|translate-never}
{(default-cost <0-16777215>|no-summary)}
area-type stub {default-cost <0-16777215> {no-summary}|no-summary
{default-cost <0-16777215>}}

```

## Parameters

`area-type nssa {default-cost|no-summary|translate-always|translate-candidate|translate-never}`

|                              |                                                                                                                                                                                                                  |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| area-type                    | Configures a particular OSPF area type as STUB, Totally STUB, NSSA or Totally NSSA                                                                                                                               |
| nssa                         | Configures the OSPF area as NSSA                                                                                                                                                                                 |
| stub                         | Configures the OSPF area as <i>Stubby Area</i> (STUB)                                                                                                                                                            |
| default-cost<br><0-16777215> | Specifies the default summary cost advertised, if the OSPF area is a STUB or NSSA <ul style="list-style-type: none"><li>&lt;0-16777215&gt; - Specify the default summary cost value from 0 - 16777215.</li></ul> |
| no-summary                   | Configures the OSPF area as totally STUB if the area-type is STUB or totally NSSA if the area-type is NSSA                                                                                                       |
| translate-always             | Always translates type-7 LSAs (Link State Advertisements) into type-5 LSAs                                                                                                                                       |
| translate-candidate          | Defines it as default behavior                                                                                                                                                                                   |
| translate-never              | Never translates type-7 LSAs into type-5 LSAs                                                                                                                                                                    |

## Examples

```
nx9500-6C8809(config-profile default-rfs4000-router-ospf-area-0.0.0.1)#area-type stub
default-cost 1
nx9500-6C8809(config-profile default-rfs4000-router-ospf-area-0.0.0.1)#show context
 area 0.0.0.1
 area-type stub default-cost 1
nx9500-6C8809(config-profile default-rfs4000-router-ospf-area-0.0.0.1)#
```

## Related Commands

|                                 |                                       |
|---------------------------------|---------------------------------------|
| <a href="#">no</a> on page 1728 | Removes configured area-type settings |
|---------------------------------|---------------------------------------|

## authentication

Specifies an authentication scheme used for an OSPF area used with the OSPF dynamic route

Supported in the following platforms:

- Access Points — AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX

## Syntax

```
authentication [message-digest|simple-password]
```

## Parameters

```
authentication [message-digest|simple-password]
```

|                 |                                                          |
|-----------------|----------------------------------------------------------|
| message-digest  | Configures a message-digest (MD-5) authentication scheme |
| simple-password | Configures a simple password authentication scheme       |

## Usage Guidelines

OSPF packet authentication enables routers to use predefined passwords and participate within a routing domain. The two authentication modes are:

- MD-5 – MD-5 authentication is a cryptographic authentication mode, where every router has a key (password) and key-id configured on it. This key and key-id together form the message digest that is appended to the OSPF packet.
- Simple Password – Simple password authentication allows a password (key) to be configured per area. Routers in the same area and participating in the routing domain have to be configured with the same key.

#### Examples

```
nx9500-6C8809(config-profile default-rfs4000-router-ospf-area-0.0.0.1)#authentication
simple-password
nx9500-6C8809(config-profile default-rfs4000-router-ospf-area-0.0.0.1)#show context
area 0.0.0.1
 authentication simple-password
 area-type stub default-cost 1
nx9500-6C8809(config-profile default-rfs4000-router-ospf-area-0.0.0.1)#
```

#### Related Commands

|                              |                                                             |
|------------------------------|-------------------------------------------------------------|
| <code>no</code> on page 1728 | Removes the authentication scheme associated with this area |
|------------------------------|-------------------------------------------------------------|

## range

Specifies a range of addresses for routes matching address/mask for OSPF summarization

Supported in the following platforms:

- Access Points – AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers – RFS 4000
- Service Platforms – NX 5500, NX 75XX

#### Syntax

```
range <IP/M>
```

#### Parameters

```
range <IP/M>
```

|        |                                                                              |
|--------|------------------------------------------------------------------------------|
| <IP/M> | Specifies the routes matching address/mask for summarization.                |
|        | <b>Note:</b> This command is applicable for a ABR (Area Border Router) only. |

#### Examples

```
nx9500-6C8809(config-profile default-rfs4000-router-ospf-area-0.0.0.1)#range 172.16.10.0/24
nx9500-6C8809(config-profile default-rfs4000-router-ospf-area-0.0.0.1)#show context
area 0.0.0.1
 authentication simple-password
 range 172.16.10.0/24
 area-type stub default-cost 1
nx9500-6C8809(config-profile default-rfs4000-router-ospf-area-0.0.0.1)#
```

#### Related Commands

|                              |                                         |
|------------------------------|-----------------------------------------|
| <code>no</code> on page 1728 | Removes the configured network IP range |
|------------------------------|-----------------------------------------|

## no

Removes this OSPF area settings

Supported in the following platforms:

- Access Points — AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX

Syntax

```
no [area-type|authentication|range]
```

Parameters

```
no <PARAMETERS>
```

|                 |                                 |
|-----------------|---------------------------------|
| no <PARAMETERS> | Removes this OSPF area settings |
|-----------------|---------------------------------|

Usage Guidelines

The **no** command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Examples

The following example shows the OSPF router settings before the 'no' commands are executed:

```
nx9500-6C8809(config-profile default-rfs4000-router-ospf-area-0.0.0.1)#show context
 area 0.0.0.1
 authentication simple-password
 range 172.16.10.0/24
 area-type stub default-cost 1
nx9500-6C8809(config-profile default-rfs4000-router-ospf-area-0.0.0.1)#
nx9500-6C8809(config-profile default-rfs4000-router-ospf-area-0.0.0.1)#no authentication
nx9500-6C8809(config-profile default-rfs4000-router-ospf-area-0.0.0.1)#no range
172.16.10.0/24
```

The following example shows the OSPF router settings after the 'no' commands are executed:

```
nx9500-6C8809(config-profile default-rfs4000-router-ospf-area-0.0.0.1)#show context
 area 0.0.0.1
 area-type stub default-cost 1
nx9500-6C8809(config-profile default-rfs4000-router-ospf-area-0.0.0.1)#
```

### *auto-cost*

Configures the reference bandwidth in terms of megabits per second. Specifying the reference bandwidth allows you to control the default metrics for an interface, which is calculated by OSPF.

The formula used to calculate default metrics is: *ref-bw* divided by the *bandwidth*.

Use the **no > auto-cost > reference-bandwidth** command to configure default metrics calculation based on interface type.

#### **Supported in the following platforms:**

- Access Points — AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000

- Service Platforms — NX 5500, NX 75XX

### Syntax

```
auto-cost reference-bandwidth <1-4294967>
```

### Parameters

```
auto-cost reference-bandwidth <1-4294967>
```

|                                    |                                                                                                                                                                         |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| reference-bandwidth<br><1-4294967> | Defines the reference bandwidth in Mbps <ul style="list-style-type: none"> <li>• &lt;1-4294967&gt; - Specify the reference bandwidth value from 1 - 4294967.</li> </ul> |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#auto-cost reference-bandwidth 1
```

Ensure that auto-cost reference-bandwidth is configured uniformly on all routers

```
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#show context router ospf
 area 0.0.0.4
 auto-cost reference-bandwidth 1
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#
```

### Related Commands

|    |                                                |
|----|------------------------------------------------|
| no | Removes auto-cost reference bandwidth settings |
|----|------------------------------------------------|

## default-information

Controls the distribution of default route information. Use the **default-information > originate** command to advertise a default route in the routing table.

This option is disabled by default. When enabled, the default route becomes a distributed route.

### Supported in the following platforms:

- Access Points — AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX

### Syntax

```
default-information originate {always|metric|metric-type}
default-information originate {always|metric <0-16777214>|metric-type [1|2]}
{(metric <0-16777214>|metric-type [1|2])}
```

### Parameters

```
default-information originate {always|metric <0-16777214>|metric-type [1|2]}
{(metric <0-16777214>|metric-type [1|2])}
```

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| originate              | Originates default route information. Enabling this feature makes the default route a distributed route. This option is disabled by default.                                                                                                                                                                                                                                                                                               |
| always                 | Optional. Always distributes default route information (will continue to advertise default route information even if that information has been removed from the routing table for some reason). This option is disabled by default.                                                                                                                                                                                                        |
| metric<br><0-16777214> | This is a recursive parameter and can be optionally configured along with the metric-type option. <ul style="list-style-type: none"> <li>metric &lt;0-16777214&gt; – Optional. Specifies OSPF metric value for redistributed routes (this value is used to generate the default route)</li> <li>&lt;0-16777214&gt; – Specify a value from 0 - 16777214.</li> </ul>                                                                         |
| metric-type [1 2]      | This is a recursive parameter and can be optionally configured along with the metric option. <ul style="list-style-type: none"> <li>metric-type [1 2] – Optional. Sets OSPF exterior metric type for redistributed routes (this information is advertised with the OSPF routing domain) <ul style="list-style-type: none"> <li>1 – Sets OSPF external type 1 metrics</li> <li>2 – Sets OSPF external type 2 metrics</li> </ul> </li> </ul> |

### Examples

```

nx9500-6C8809(config-profile default-rfs4000-router-ospf)#default-information
originate metric-type 2 metric 1
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#show context
router ospf
 area 0.0.0.4
 auto-cost reference-bandwidth 1
 default-information originate metric 1 metric-type 2
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#

```

### Related Commands

|           |                                                                                  |
|-----------|----------------------------------------------------------------------------------|
| <b>no</b> | Disables advertising of default route information available in the routing table |
|-----------|----------------------------------------------------------------------------------|

*ip*

Configures IP default gateway priority

### Supported in the following platforms:

- Access Points — AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX

### Syntax

```
ip default-gateway priority <1-8000>
```

### Parameters

```
ip default-gateway priority <1-8000>
```

|                   |                                                                                                                                                                                                                                                      |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| default-gateway   | Configures the default gateway                                                                                                                                                                                                                       |
| priority <1-8000> | Sets the priority for the default gateway acquired via OSPF <ul style="list-style-type: none"> <li>• &lt;1-8000&gt; – Specify an integer from 1 - 8000. The default is 7000.</li> </ul> <p><b>Note:</b> Lower the value, higher is the priority.</p> |

### Examples

```

nx9500-6C8809(config-profile default-rfs4000-router-ospf)#ip default-gateway priority 1
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#show context
router ospf
 area 0.0.0.4
 auto-cost reference-bandwidth 1
 default-information originate metric 1 metric-type 2
 ip default-gateway priority 1
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#

```

### Related Commands

|    |                                           |
|----|-------------------------------------------|
| no | Removes default gateway priority settings |
|----|-------------------------------------------|

## network

Assigns networks to specified areas (defines the OSPF interfaces and their associated area IDs)

### Supported in the following platforms:

- Access Points — AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX

### Syntax

```
network <IP/M> area [<0-4294967295>|<IP>]
```

### Parameters

```
network <IP/M> area [<0-4294967295>|<IP>]
```

|                            |                                                                                                                                                                                                                                                                                                                |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IP/M>                     | Specifies an OSPF network address/mask value. Defines networks (IP addresses and mask) participating in OSPF.                                                                                                                                                                                                  |
| area [<0-4294967295> <IP>] | Specifies an OSPF area, associated with the OSPF address range, in one of the following formats: <ul style="list-style-type: none"> <li>• &lt;0-4294967295&gt; – Specifies a 32 bit OSPF area ID from 0 - 4294967295</li> <li>• &lt;IP&gt; – Defines an OSPF area ID in the form of an IPv4 address</li> </ul> |

### Examples

```

nx9500-6C8809(config-profile default-rfs4000-router-ospf)#network 1.2.3.0/24 area 4.5.6.7
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#show context
router ospf
 network 1.2.3.0/24 area 4.5.6.7
 area 0.0.0.4
 auto-cost reference-bandwidth 1
 default-information originate metric 1 metric-type 2

```

```
ip default-gateway priority 1
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#
```

### Related Commands

|                 |                                                 |
|-----------------|-------------------------------------------------|
| <code>no</code> | Removes the OSPF network to area ID association |
|-----------------|-------------------------------------------------|

### *ospf*

Enables OSPF routing on a profile or device

#### Supported in the following platforms:

- Access Points — AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX

#### Syntax

```
ospf enable
```

#### Parameters

```
ospf enable
```

|                          |                                                                                         |
|--------------------------|-----------------------------------------------------------------------------------------|
| <code>ospf enable</code> | Enables OSPF routing on devices using this profile. This option is disabled by default. |
|--------------------------|-----------------------------------------------------------------------------------------|

#### Examples

```
cnx9500-6C8809(config-profile default-rfs4000-router-ospf)#ospf enable
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#show context
router ospf
 ospf enable
 network 1.2.3.0/24 area 4.5.6.7
 area 0.0.0.4
 auto-cost reference-bandwidth 1
 default-information originate metric 1 metric-type 2
 ip default-gateway priority 1
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#
```

### Related Commands

|                 |                                              |
|-----------------|----------------------------------------------|
| <code>no</code> | Disables OSPF routing on a profile or device |
|-----------------|----------------------------------------------|

### *passive*

Configures specified OSPF interface as passive. This option is disabled by default.

A passive interface receives routing updates, but does not transmit them.

#### Supported in the following platforms:

- Access Points — AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000



- Service Platforms — NX 5500, NX 75XX

### Syntax

```
passive [<WORD>|all|vlan <1-4094>]
```

### Parameters

```
passive [<WORD>|all|vlan <1-4094>]
```

|               |                                                                                                                                                                                 |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <WORD>        | Enables the OSPF passive mode on the interface specified by the <WORD> parameter                                                                                                |
| all           | Enables the OSPF passive mode on all the L3 interfaces                                                                                                                          |
| vlan <1-4094> | Enables the OSPF passive mode on the specified VLAN interface <ul style="list-style-type: none"> <li>• &lt;1-4094&gt; – Specify the VLAN interface ID from 1 - 4094.</li> </ul> |

### Examples

```
cnx9500-6C8809(config-profile default-rfs4000-router-ospf)#passive vlan 1
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#show context
router ospf
 ospf enable
 network 1.2.3.0/24 area 4.5.6.7
 area 0.0.0.4
 auto-cost reference-bandwidth 1
 default-information originate metric 1 metric-type 2
 passive vlan1
 ip default-gateway priority 1
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#
```

### Related Commands

|           |                                                         |
|-----------|---------------------------------------------------------|
| <b>no</b> | Disables the OSPF passive mode on a specified interface |
|-----------|---------------------------------------------------------|

### *redistribute*

Specifies the route types redistributed by OSPF

### Supported in the following platforms:

- Access Points — AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX

### Syntax

```
redistribute [bgp|connected|kernel|static] {metric <0-16777214>|metric-type [1|2]}
```

### Parameters

```
redistribute [bgp|connected|kernel|static] {metric <0-16777214>|metric-type [1|2]}
```

|           |                                                                              |
|-----------|------------------------------------------------------------------------------|
| bgp       | Redistributes all BGP routes by OSPF                                         |
| connected | Redistributes all connected interface routes by OSPF                         |
| kernel    | Redistributes all routes that are neither connected, nor static, nor dynamic |

|                     |                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| static              | Redistributes static routes by OSPF                                                                                                                                                                                                                                                                                                                                                  |
| metric <0-16777214> | The following keywords are common to the 'bgp', 'connected', 'kernel', and 'static' parameters: <ul style="list-style-type: none"> <li>metric &lt;0-16777214&gt; – Optional. Specifies the OSPF metric value for redistributed routes.</li> <li>&lt;0-16777214&gt; – Specify a value from 0 - 16777214.</li> </ul>                                                                   |
| metric-type[1 2]    | The following keywords are common to the 'connected', 'kernel', and 'static' parameters: <ul style="list-style-type: none"> <li>metric-type [1 2] – Optional. Sets the OSPF exterior metric type for redistributed routes <ul style="list-style-type: none"> <li>1 – Sets the OSPF external type 1 metrics</li> <li>2 – Sets the OSPF external type 2 metrics</li> </ul> </li> </ul> |

### Examples

```

nx9500-6C8809(config-profile default-rfs4000-router-ospf)#redistribute static metric-type 1
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#show context
router ospf
 ospf enable
 network 1.2.3.0/24 area 4.5.6.7
 area 0.0.0.4
 auto-cost reference-bandwidth 1
 default-information originate metric 1 metric-type 2
 redistribute static metric-type 1
 passive vlan1
 ip default-gateway priority 1
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#

```

### Related Commands

|    |                                                        |
|----|--------------------------------------------------------|
| no | Removes the OSPF redistribution of various route types |
|----|--------------------------------------------------------|

### route-limit

Limits the number of routes managed by OSPF. The maximum limit supported by the platform is the default configuration defined under the router-ospf context.

#### Supported in the following platforms:

- Access Points — AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX

#### Syntax

```

route-limit [num-routes|reset-time|retry-count|retry-timeout]
route-limit [num-routes <DYNAMIC-ROUTE-LIMIT>|reset-time <1-86400>|retry-count <1-32>|
retry-timeout <1-3600>] {(num-routes|reset-time|retry-count|retry-timeout)}

```

#### Parameters

```

route-limit [num-routes <DYNAMIC-ROUTE-LIMIT>|reset-time <1-86400>|retry-count <1-32>|
retry-timeout <1-3600>] {(num-routes|reset-time|retry-count|retry-timeout)}

```

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| num-routes<br><DYNAMIC-ROUTE-LIMIT> | Specifies the maximum number of non self-generated LSAs this process can receive <ul style="list-style-type: none"> <li>• &lt;DYNAMIC-ROUTE-LIMIT&gt; - Specify the dynamic route limit.</li> </ul>                                                                                                                                                                                                                                          |
| reset-time<br><1-86400>             | Specifies the time, in seconds, after which the retry-count is reset to zero <ul style="list-style-type: none"> <li>• &lt;1-86400&gt; - Specify a value from 1 - 86400 seconds. The default is 360 seconds.</li> </ul>                                                                                                                                                                                                                       |
| retry-count <1-32>                  | Specifies the maximum number of times adjacencies can be suppressed. Each time OSPF gets into an ignore state, a counter increments. If the counter exceeds the timeout configured by the retry-count parameter, OSPF stays in the same ignore state. Manual intervention is required to get OSPF out of the ignore state. <ul style="list-style-type: none"> <li>• &lt;1-32&gt; - Specify a value from 1 - 32. The default is 5.</li> </ul> |
| retry-timeout<br><1-3600>           | Specifies the retry time in seconds. During this time, OSPF remains in ignore state and all adjacencies are suppressed. <ul style="list-style-type: none"> <li>• &lt;1-3600&gt; - Specify a value from 1 - 3600 seconds. The default is 60 seconds.</li> </ul>                                                                                                                                                                               |

### Examples

```

cnx9500-6C8809(config-profile default-rfs4000-router-ospf)#route-limit num-routes 10
retry-count 5 retry-timeout 60 reset-time 10
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#show context
router ospf
 ospf enable
 network 1.2.3.0/24 area 4.5.6.7
 area 0.0.0.4
 auto-cost reference-bandwidth 1
 default-information originate metric 1 metric-type 2
 redistribute static metric-type 1
 passive vlan1
 route-limit num-routes 10 retry-count 5 retry-timeout 60 reset-time 10
 ip default-gateway priority 1
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#

```

### Related Commands

|           |                                                           |
|-----------|-----------------------------------------------------------|
| <b>no</b> | Removes the limit on the number of routes managed by OSPF |
|-----------|-----------------------------------------------------------|

### *router-id*

Specifies the OSPF router ID

This ID must be established in every OSPF instance. If not explicitly configured, the highest logical IP address is duplicated as the router identifier. However, since the router identifier is not an IP address, it does not have to be a part of any routable subnet in the network.

### Supported in the following platforms:

- Access Points — AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX

### Syntax

```
router-id <IP>
```

## Parameters

router-id <IP>

|      |                                                                                                                                                                    |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IP> | Identifies the OSPF router by its IP address <ul style="list-style-type: none"><li>• &lt;IP&gt; - Specify the router ID in the IP &lt;A.B.C.D&gt; format</li></ul> |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#router-id 172.16.10.8
```

Reload, or execute "clear ip ospf process" command, for this to take effect

```
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#
```

## Related Commands

|    |                                       |
|----|---------------------------------------|
| no | Removes the configured OSPF router ID |
|----|---------------------------------------|

no

Removes this OSPF router settings or reverts them to default values

## Supported in the following platforms:

- Access Points — AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX

## Syntax

```
no [area|auto-cost|default-information|ip|network|ospf|passive|redistribute|route-limit|router-id]
```

## Parameters

no <PARAMETERS>

|                 |                                       |
|-----------------|---------------------------------------|
| no <PARAMETERS> | Negates a command or set its defaults |
|-----------------|---------------------------------------|

## Usage Guidelines

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

## Examples

The following example shows the OSPF router interface settings before the 'no' commands are executed:

```
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#show context
router ospf
 network 1.2.3.0/24 area 4.5.6.7
 area 0.0.0.4
 auto-cost reference-bandwidth 1
 default-information originate metric 1 metric-type 2
 redistribute static metric-type 1
 passive vlan1
```

---

```
route-limit num-routes 10 reset-time 10
ip default-gateway priority 1
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#no area 4
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#no auto-cost reference-bandwidth
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#no network 1.2.3.0/24 area
4.5.6.7
```

The following example shows the OSPF router interface settings after the 'no' commands are executed:

```
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#show context
router ospf
 default-information originate metric 1 metric-type 2
 redistribute static metric-type 1
 passive vlan1
 route-limit num-routes 10 reset-time 10
 ip default-gateway priority 1
nx9500-6C8809(config-profile default-rfs4000-router-ospf)#
```

# Routing Policy

## ROUTING-POLICY

---

This chapter summarizes routing-policy commands in the CLI command structure.

Routing policies enable network administrators to control data packet routing and forwarding. PBR (Policy-based routing) always overrides protocol-based routing. Network administrators can define routing policies based on parameters, such as access lists, packet size etc. For example, a routing policy can be configured to route packets along user-defined routes.

In addition to the above, PBR policies facilitate the provisioning of preferential service to specific traffic. PBR minimally provides the following:

- A means to use source address, protocol, application and traffic class as traffic routing criteria
- A means to load balance multiple WAN uplinks
- A means to selectively mark traffic for QoS (Quality of Service) optimization

Use the (config) instance to configure router-policy commands. To navigate to the (config-routing-policy mode) instance, use the following commands:

```
<DEVICE>(config)#routing-policy <ROUTING-POLICY-NAME>
nx9500-6C8809(config)#routing-policy testpolicy
nx9500-6C8809(config-routing-policy-testpolicy)#?
Routing Policy Mode commands:
 apply-to-local-packets Use Policy Based Routing for packets generated by
 the device
 logging Enable logging for this Route Map
 no Negate a command or set its defaults
 route-map Create a Route Map
 use Set setting to use

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-routing-policy-testpolicy)#
```

### routing-policy-commands

The following table summarizes routing policy configuration mode commands:

**Table 59: Routing-Policy-Config Commands**

| Command                             | Description                               |
|-------------------------------------|-------------------------------------------|
| <code>apply-to-local-packets</code> | Enables PBR for locally generated packets |
| <code>logging</code>                | Enables logging for a specified route map |
| <code>route-map</code>              | Creates a route map entry                 |
| <code>use</code>                    | Defines default settings to use           |
| <code>no</code>                     | Negates a command or sets its defaults    |

**Note**

For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see [COMMON COMMANDS](#) on page 640.

**Note**

The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (\_) character. In other words, the name of a device cannot contain an underscore.

*apply-to-local-packets*

Enables PBR for locally generated packets (packets generated by the device). When enabled, this option implements the match and action clauses defined within route maps. This option is enabled by default.

**Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

**Syntax**

```
apply-to-local-packets
```

**Parameters**

None

**Examples**

```
nx9500-6C8809(config-routing-policy-testpolicy)#apply-to-local-packets
nx9500-6C8809(config-routing-policy-testpolicy)#
```

**Related Commands**

|                 |                                            |
|-----------------|--------------------------------------------|
| <code>no</code> | Disables PBR for locally generated packets |
|-----------------|--------------------------------------------|

## logging

Enables logging for a specified route map. When enabled, this option logs events generated by the enforcement of route-maps. This option is disabled by default.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

logging

### Parameters

None

### Examples

```
nx9500-6C8809(config-routing-policy-testpolicy)#logging
nx9500-6C8809(config-routing-policy-testpolicy)#show context
routing-policy testpolicy
 logging
nx9500-6C8809(config-routing-policy-testpolicy)#
```

### Related Commands

|                 |                            |
|-----------------|----------------------------|
| no on page 1749 | Disables route map logging |
|-----------------|----------------------------|

## route-map

Creates a route map entry and enters the route map configuration mode

In PBR, route maps control the flow of traffic within the network. They override route tables and direct traffic along a specific path.

Route-maps contain a set of filters that select traffic (match clauses) and associated actions (mark clauses) for routing. Every route-map entry has a precedence value. Lower the precedence, higher is the route-map's priority. All incoming packets are matched against these route-maps entries. The route-map entry with highest precedence (lowest numerical value) is applied first. In case of a match, action is taken based on the mark clause specified in the route-map. In case of no match, the route-map entry with the next highest precedence is applied. If the incoming packet does not match any of the route-map entries, it is subjected to typical destination-based routing. Each route-map entry can optionally enable/disable logging.

The following criteria can optionally be used as traffic selection segregation criteria:

- *IP Access List* - A typical IP ACL can be used for routing traffic. The mark and log actions in ACL rules however are neglected. Route-map entries have separate logging. Only one ACL can be configured per route map entry.



---

ACL rules configured under route map entries merge to create a single ACL. Route map precedence values determine the prioritization of the rules in this merged ACL. An IP DSCP value is also added to the ACL rules.

- *IP DSCP* - Packet filtering can be performed by traffic class, as determined from the IP DSCP (Differentiated Services Code Point) field. One DSCP value can be configured per route map entry. If IP ACLs on a WLAN, ports or SVI mark packets, the new/marked DSCP value is used for matching.
- *Incoming WLAN* - Packets can be filtered on the basis of the incoming WLAN. Depending on whether the receiving device has an onboard radio or not, the following two scenarios are possible:
  - Device with an onboard radio: If a device having an onboard radio and capable of PBR receives a packet on a local WLAN, this WLAN is used for selection.
  - Device without an onboard radio: If a device, without an onboard radio, capable of PBR receives a packet from an extended VLAN, it passes the WLAN information in the MiNT packet to the PBR router. The PBR router uses this information as match criteria.
- *Client role* - The client role can be used as match criteria, similar to a WLAN. Each device has to agree on a unique identifier for role definition and pass the same MINT tunneled packets.
- *Incoming SVI* - A source IP address qualifier in an ACL typically satisfies filter requirements. But if the source host (where the packet originates) is multiple hops away, the incoming SVI can be used as match criteria. In this context the SVI refers to the device interface performing PBR, and not to the source device.

Mark (or action) clauses determine the routing function when a packet satisfies match criteria. If no mark clauses are defined, the default is to fallback to destination-based routing for packets satisfying the match criteria. If no mark clause is configured and fallback to destination-based routing is disabled, then the packet is dropped. The mark clause defines one of following actions:

- *Next hop* - The IP address of the next hop or the outgoing interface through which the packet should be routed. Up to two next hops can be specified. The outgoing interface should be a PPP, a tunnel interface or a SVI which has DHCP client configured. The first reachable hop should be used. But if all next hops are unreachable, typical destination-based route lookup is performed.
- *Default next hop* - If a packet subjected to PBR does not have an explicit route to the destination, the configured default next hop is used. This can be either the IP address of the next hop or the outgoing interface. Only one default next hop can be defined. The difference between the next hop and the default next-hop is: in case of the former, PBR occurs first, then destination-based routing. In case of the latter, the order is reversed. In both cases:
  - 1 If a defined next hop is reachable, it is used. If fallback is configured refer to (b).
  - 2 Perform normal destination-based route lookup. If a next hop is found, it is used, if not refer to (c).
  - 3 If default next hop is configured and reachable, it is used, if not, packet is dropped.
- *Fallback* - Enables fallback to destination-based routing if none of the configured next hops are reachable (or not configured). This is enabled by default.
- *Mark IP DSCP* - Configures IP DSCP bits for QoS using an ACL. The mark action of the route maps takes precedence over the mark action of an ACL.

#### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000

- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
route-map <1-100>
```

## Parameters

```
route-map <1-100>
```

|                   |                                                                                                                                                                                                                                                                                                         |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| route-map <1-100> | Creates a route map entry, sets a precedence value for the route map, and enters the route map configuration mode <ul style="list-style-type: none"> <li>• &lt;1-100&gt; - Specify a precedence value from 1 - 100.</li> </ul> <p><b>Note:</b> Lower the sequence number, higher is the precedence.</p> |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
<DEVICE>(config-routing-policy-testpolicy)#route-map 1
nx9500-6C8809(config-routing-policy-testpolicy)#show context
routing-policy testpolicy
 logging
 route-map 1
nx9500-6C8809(config-routing-policy-testpolicy)#
nx9500-6C8809(config-routing-policy-testpolicy)#route-map 1
nx9500-6C8809(config-routing-policy-testpolicy-route-map-1)#?
Route Map Mode commands:
 default-next-hop Default next-hop configuration (aka
 gateway-of-last-resort)
 fallback Fallback to destination based routing if no next-hop is
 configured or all are unreachable
 mark Mark action for route map
 match Match clause configuration for Route Map
 next-hop Next-hop configuration
 no Negate a command or set its defaults

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-routing-policy-testpolicy-route-map-1)#
```

## Related Commands

The following table summarizes route-map configuration mode commands:

**Table 60: Route-Map-Config Commands**

| Command          | Description                                                     |
|------------------|-----------------------------------------------------------------|
| default-next-hop | Sets the default next hop for packets satisfying match criteria |
| fallback         | Configures a fallback to the next destination                   |
| mark             | Marks action clause for packets satisfying match criteria       |

**Table 60: Route-Map-Config Commands (continued)**

| Command                                                   | Description                                                      |
|-----------------------------------------------------------|------------------------------------------------------------------|
| <code>match</code>                                        | Sets match clauses for the route map                             |
| <code>next-hop</code>                                     | Sets the next hop for packets satisfying match criteria          |
| <code>no</code> (route-map config mode 'no' command)      | Removes the route-map settings or reverts them to default values |
| <code>no</code> (routing-policy config mode 'no' command) | Removes a route map from the routing policy                      |

**default-next-hop**

Sets the default next hop for packets satisfying match criteria.

If a packet, subjected to PBR, does not have an explicit route to the destination, the configured default next hop is used. This value is set as either the IP address of the next hop or the outgoing interface. Only one default next hop can be defined. The difference between the next hop and the default next-hop is: in case of the former, PBR occurs first, then destination-based routing. In case of the latter, the order is reverse. Use this command to set either the default next hop IP address or define either a WWAN1, PPPoE1, or VLAN interface.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

**Syntax**

```
default-next-hop [<IP> | <ROUTER-IF-NAME> | pppoe1 | serial <SLOT-ID> <PORT-ID>
<CHANNEL-GROUP-ID> | vlan <1-4094> | wwan1]
```

**Parameters**

```
default-next-hop [<IP> | <ROUTER-IF-NAME> | pppoe1 | serial <SLOT-ID> <PORT-ID>
<CHANNEL-GROUP-ID> | vlan <1-4094> | wwan1]
```

|                                                                              |                                                                                                                                                |
|------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>default-next--hop</code>                                               | Sets the next hop router to which packets are sent in case the next hop is not the adjacent router                                             |
| <code>&lt;IP&gt;</code>                                                      | Specifies next hop router's IP address                                                                                                         |
| <code>&lt;ROUTER-IF-NAME&gt;</code>                                          | Specifies the outgoing interface name (router interface name)                                                                                  |
| <code>pppoe1</code>                                                          | Specifies the PPPoE interface                                                                                                                  |
| <code>serial &lt;SLOT-ID&gt; &lt;PORT-ID&gt; &lt;CHANNEL-GROUP-ID&gt;</code> | Specifies the serial interface's slot, port, and channel group IDs                                                                             |
| <code>vlan &lt;1-4094&gt;</code>                                             | Specifies a VLAN interface ID <ul style="list-style-type: none"> <li>• <code>&lt;1-4094&gt;</code> - Specify a value from 1 - 4094.</li> </ul> |
| <code>wwan1</code>                                                           | Specifies the WAN interface                                                                                                                    |

## Examples

```
nx9500-6C8809(config-routing-policy-testpolicy-route-map-1)#default-next-hop wwan1
nx9500-6C8809(config-routing-policy-testpolicy-route-map-1)#show context
 route-map 1
 default-next-hop wwan1
nx9500-6C8809(config-routing-policy-testpolicy-route-map-1)#
```

## Related Commands

|    |                                          |
|----|------------------------------------------|
| no | Removes default next hop router settings |
|----|------------------------------------------|

## fallback

Enables fallback to destination-based routing. This option is enabled by default. To disable fallback, use the `no > fallback` command.

The action taken for packets satisfying the match criteria is determined by the mark (action) clauses. If no action is defined, the default is to fallback to destination-based routing.



### Note

If no mark clause is configured and fallback to destination-based routing is disabled, then the packet is dropped.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
fallback
```

## Parameters

None

## Examples

```
nx9500-6C8809(config-routing-policy-testpolicy-route-map-1)#fallback
nx9500-6C8809(config-routing-policy-testpolicy-route-map-1)#
```

## Related Commands

|    |                                                                                                |
|----|------------------------------------------------------------------------------------------------|
| no | Disables fallback to destination-based routing if no next hop is configured or are unreachable |
|----|------------------------------------------------------------------------------------------------|

## mark

Enables the marking of the DSCP field in the IP header

Use this command to set the IP DSCP bits for QoS using an ACL. The mark action of the route maps takes precedence over the mark action of an ACL.

The DSCP field in an IP header enables packet classification. Packet filtering can be done based on traffic class, determined from the IP DSCP field. One DSCP value can be configured per route map entry.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
mark ip dscp <0-63>
```

#### Parameters

```
mark ip dscp <0-63>
```

|                |                                                                                                                                            |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| ip dscp <0-63> | Marks the DSCP field in the IP header <ul style="list-style-type: none"> <li>• &lt;0-63&gt; - Specify a DSCP value from 0 - 63.</li> </ul> |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config-routing-policy-testpolicy-route-map-1)#mark ip dscp 7
nx9500-6C8809(config-routing-policy-testpolicy-route-map-1)#show context
route-map 1
 default-next-hop wwan1
 mark ip dscp 7
nx9500-6C8809(config-routing-policy-testpolicy-route-map-1)#
```

#### Related Commands

|    |                                |
|----|--------------------------------|
| no | Disables marking of IP packets |
|----|--------------------------------|

## match

Sets the match clauses

Each route map entry has a set of match clauses used to segregate and filter packets. Packets can be segregated using any one of the following criteria:

- *IP Access List* - A typical IP ACL can be used for routing traffic. The mark and log actions in ACL rules however are neglected. Route-map entries have separate logging. Only one ACL can be configured per route map entry.

ACL rules configured under route map entries merge to create a single ACL. Route map precedence values determine the prioritization of the rules in this merged ACL. An IP DSCP value is also added to the ACL rules.

- *IP DSCP* - Packet filtering can be performed by traffic class, as determined from the IP Differentiated Services Code Point (DSCP) field. One DSCP value can be configured per route map entry. If IP ACLs on a WLAN, ports or SVI mark packets, the new/marked DSCP value is used for matching.
- *Incoming WLAN* - Packets can be filtered on the basis of the incoming WLAN. Depending on whether the receiving device has an onboard radio or not, the following two scenarios are possible:
  - Device with an onboard radio: If a device having an onboard radio and capable of PBR receives a packet on a local WLAN, this WLAN is used for selection.
  - Device without an onboard radio: If a device, without an onboard radio, capable of PBR receives a packet from an extended VLAN, it passes the WLAN information in the MiNT packet to the PBR router. The PBR router uses this information as match criteria.

- *Client role* - The client role can be used as match criteria, similar to a WLAN. Each device has to agree on a unique identifier for role definition and pass the same MINT tunneled packets.
- *Incoming SVI* - A source IP address qualifier in an ACL typically satisfies filter requirements. But if the source host (where the packet originates) is multiple hops away, the incoming SVI can be used as match criteria. In this context the SVI refers to the device interface performing PBR, and not to the source device.

The action taken for filtered packets is determined by the mark (action) clauses. If no action is defined, the default is to fallback to destination-based routing for packets satisfying the match criteria. For more information on configuring mark clauses, see [mark](#) on page 1744. And for more information on fallback action, see [fallback](#) on page 1744.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
match [incoming-interface|ip|ip-access-list|wireless-client-role|wlan]
match incoming-interface [<ROUTER-IF-NAME>|pppoe1|serial <SLOT-ID> <PORT-ID>
<CHANNEL-GROUP-ID>|vlan <1-4094>|wwan1]
match ip dscp <0-63>
match ip-access-list <IP-ACCESS-LIST-NAME>
match wireless-client-role <ROLE-POLICY-NAME> <ROLE-NAME>
match wlan <WLAN-NAME>
```

### Parameters

```
match incoming-interface [<ROUTER-IF-NAME>|pppoe1|serial <SLOT-ID> <PORT-ID>
<CHANNEL-GROUP-ID>|vlan <1-4094>|wwan1]
```

|                                                  |                                                                                                                                       |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| incoming-interface                               | Sets the incoming SVI match clause. Specify an interface name.                                                                        |
| <ROUTER-IF-NAME>                                 | Specifies the layer 3 interface name (route interface)                                                                                |
| pppoe1                                           | Specifies the PPP over Ethernet interface                                                                                             |
| serial <SLOT-ID> <PORT-ID><br><CHANNEL-GROUP-ID> | Specifies the serial interface's slot, port, and channel group IDs.                                                                   |
| vlan <1-4094>                                    | Specifies the VLAN interface ID <ul style="list-style-type: none"> <li>• &lt;1-4094&gt; - Specify a VLAN ID from 1 - 4094.</li> </ul> |
| wwan1                                            | Specifies the WAN interface name                                                                                                      |

```
match ip dscp <0-63>
```

|                |                                                                                                                                                                                                    |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip dscp <0-63> | Sets the DSCP match clause <ul style="list-style-type: none"> <li>• &lt;0-63&gt; - Specify a value from 0 - 63. The defined DSCP value is used as a matching clause for this route map.</li> </ul> |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
match ip-access-list <IP-ACCESS-LIST-NAME>
```

|                                                         |                                                                                                                                                                                           |
|---------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>ip-access-list &lt;IP-ACCESS-LIST-NAME&gt;</code> | Sets the match clause using a pre-configured IP access list <ul style="list-style-type: none"><li>• &lt;IP-ACCESS-LIST-NAME&gt; – Specify a pre-configured IP access list name.</li></ul> |
|---------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

`match wireless-client-role <ROLE-POLICY-NAME> <ROLE-NAME>`

|                                                                              |                                                                                                                                                                                                                                      |
|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>wireless-client-role &lt;ROLE-POLICY-NAME&gt; &lt;ROLE-NAME&gt;</code> | Sets the wireless client role match clause <ul style="list-style-type: none"><li>• &lt;ROLE-POLICY-NAME&gt; – Specify a pre-configured role policy.</li><li>• &lt;ROLE-NAME&gt; – Specify a pre-configured role within it.</li></ul> |
|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

`match wlan <WLAN-NAME>`

|                                     |                                                                                                                                |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <code>wlan &lt;WLAN-NAME&gt;</code> | Sets the incoming WLAN match clause <ul style="list-style-type: none"><li>• &lt;WLAN-NAME&gt; – Specify a WLAN name.</li></ul> |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config-routing-policy-testpolicy-route-map-1)#match incoming-interface pppoe1
nx9500-6C8809(config-routing-policy-testpolicy-route-map-1)#show context
route-map 1
 match incoming-interface pppoe1
 default-next-hop wwan1
 mark ip dscp 7
nx9500-6C8809(config-routing-policy-testpolicy-route-map-1)#
```

### Related Commands

|                 |                                                   |
|-----------------|---------------------------------------------------|
| <code>no</code> | Disables match clause settings for this route map |
|-----------------|---------------------------------------------------|

## next-hop

Sets the next hop for packets satisfying match criteria

This command allows you to configure the primary and secondary hop priority requests.

Define the primary and secondary hop settings. When defined, the primary hop resource is used with no additional considerations when ever it is available.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
next-hop [<IP>|<ROUTER-IF-NAME>|pppoe1|serial <SLOT-ID> <PORT-ID> <CHANNEL-GROUP-ID>|
vlan <1-4094>|wwlan1] {<IP>|<ROUTER-IF-NAME>|pppoe1|serial <SLOT-ID> <PORT-ID>
<CHANNEL-GROUP-ID>|vlan <1-4094>|wwlan1}
```

### Parameters

```
next-hop [<IP>|<ROUTER-IF-NAME>|pppoe1|serial <SLOT-ID> <PORT-ID> <CHANNEL-GROUP-ID>|
vlan <1-4094>|wwlan1] {<IP>|<ROUTER-IF-NAME>|pppoe1|serial <SLOT-ID> <PORT-ID>
<CHANNEL-GROUP-ID>|vlan <1-4094>|wwlan1}
```

|                                               |                                                                                                                                                                                                                                  |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| next-hop                                      | Sets the next hop (primary and secondary) for packets satisfying match criteria<br><br><b>Note:</b> It is not mandatory to define the secondary hop interface. The secondary hop is used in case the primary hop is unavailable. |
| <IP>                                          | Specifies the primary and secondary next hop router's IP address                                                                                                                                                                 |
| <WORD>                                        | Specifies the layer 3 Interface name (router interface)                                                                                                                                                                          |
| pppoe1                                        | Specifies the PPP over Ethernet interface                                                                                                                                                                                        |
| serial <SLOT-ID> <PORT-ID> <CHANNEL-GROUP-ID> | Specifies the serial interface's slot, port, and channel group IDs.                                                                                                                                                              |
| vlan <1-4094>                                 | Specifies the VLAN interface ID <ul style="list-style-type: none"> <li>• &lt;1-4094&gt; – Specify a VLAN ID from 1 - 4094. The VLAN interface should be a DHCP client.</li> </ul>                                                |
| wwan1                                         | Specifies the WAN interface                                                                                                                                                                                                      |

### Examples

```

nx9500-6C8809(config-routing-policy-testpolicy-route-map-1)#next-hop vlan 1
nx9500-6C8809(config-routing-policy-testpolicy-route-map-1)#show context
route-map 1
 match incoming-interface pppoe1
 next-hop vlan1
 default-next-hop wwan1
 mark ip dscp 7
nx9500-6C8809(config-routing-policy-testpolicy-route-map-1)#

```

### Related Commands

|    |                                       |
|----|---------------------------------------|
| no | Disables the next hop router settings |
|----|---------------------------------------|

## no

Removes this route-map settings or reverts them to default values

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
no [default-next-hop|fallback|mark|match|next-hop]
```

### Parameters

```
no <PARAMETERS>
```

|                 |                                                                                                   |
|-----------------|---------------------------------------------------------------------------------------------------|
| no <PARAMETERS> | Removes this route-map settings or reverts them to default values, based on the parameters passed |
|-----------------|---------------------------------------------------------------------------------------------------|

### Usage Guidelines

The **no** command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.



## Examples

The following example shows the route-map '1' settings before the 'no' commands are executed:

```
nx9500-6C8809(config-routing-policy-testpolicy-route-map-1)#show context
route-map 1
 match incoming-interface pppoe1
 next-hop vlan1
 default-next-hop wwan1
 mark ip dscp 7
nx9500-6C8809(config-routing-policy-testpolicy-route-map-1)#
nx9500-6C8809(config-routing-policy-testpolicy-route-map-1)#no default-next-hop
nx9500-6C8809(config-routing-policy-testpolicy-route-map-1)#no next-hop
```

The following example shows the route-map '1' settings after the 'no' commands are executed:

```
nx9500-6C8809(config-routing-policy-testpolicy-route-map-1)#show context
route-map 1
 match incoming-interface pppoe1
 mark ip dscp 7
nx9500-6C8809(config-routing-policy-testpolicy-route-map-1)#
```

## use

Uses CRM (Critical Resource Monitoring) to monitor link status

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
use critical-resource-monitoring
```

### Parameters

```
use critical-resource-monitoring
```

|                                  |                                                                                                                                                                                                                                                                                              |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| use critical-resource-monitoring | Uses CRM to monitor the status of a link. Selecting this option determines the disposition of the route-map next hop via monitored critical resources. Link monitoring is the function used to determine a potential fail over to the secondary next hop. This option is enabled by default. |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config-routing-policy-testpolicy)#use critical-resource-monitoring
nx9500-6C8809(config-routing-policy-testpolicy)#
```

### Related Commands

|    |                                     |
|----|-------------------------------------|
| no | Disables CRM link status monitoring |
|----|-------------------------------------|

## no

Removes this Routing policy settings or reverts them to default values

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
no [apply-to-local-packets|logging|route-map|use]
```

### Parameters

```
no <PARAMETERS>
```

|                 |                                                                                                         |
|-----------------|---------------------------------------------------------------------------------------------------------|
| no <PARAMETERS> | Removes this routing policy settings or reverts them to default values, based on the parameters passed. |
|-----------------|---------------------------------------------------------------------------------------------------------|

### Usage Guidelines

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

### Examples

The following example shows the routing policy 'testpolicy' settings before the 'no' commands are executed:

```
nx9500-6C8809(config-routing-policy-testpolicy)#show context
routing-policy testpolicy
 logging
 route-map 1
 match incoming-interface pppoe1
 default-next-hop wwan1 mark ip dscp 7
nx9500-6C8809(config-routing-policy-testpolicy)#
nx9500-6C8809(config-routing-policy-testpolicy)#no logging
nx9500-6C8809(config-routing-policy-testpolicy)#no route-map 1
nx9500-6C8809(config-routing-policy-testpolicy)#no apply-to-local-packets
```

The following example shows the routing policy 'testpolicy' settings after the 'no' commands are executed:

```
nx9500-6C8809(config-routing-policy-testpolicy)#show context
routing-policy testpolicy
 no apply-to-local-packets
nx9500-6C8809(config-routing-policy-testpolicy)#
```

# AAA TACACS POLICY COMMANDS

## AAA-TACACS-POLICY

---

This chapter summarizes the AAA (accounting, authentication, and authorization) TACACS (Terminal Access Control Access-Control System) policy commands in the CLI command structure.

TACACS is a network security application that provides additional network security by providing a centralized authentication, authorization, and accounting platform. TACACS implementation requires configuration of the TACACS authentication server and database.

Use the (config) instance to configure AAA-TACACS policy commands. To navigate to the config-aaa-tacacs-policy instance, use the following commands:

```
<DEVICE>(config)#aaa-tacacs-policy <POLICY-NAME>
nx9500-6C8809(config)#aaa-tacacs-policy test
nx9500-6C8809(config-aaa-tacacs-policy-test)#?
AAA TACACS Policy Mode commands:
 accounting Configure accounting parameters
 authentication Configure authentication parameters
 authorization Configure authorization parameters
 no Negate a command or set its defaults

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-aaa-tacacs-policy-test)#
```

### aaa-tacacs-policy-commands

The following table summarizes the AAA TACACS policy configuration mode commands:

**Table 61: AAA TACACS Policy Configuration Commands**

| Command        | Description                                 |
|----------------|---------------------------------------------|
| accounting     | Configures TACACS accounting parameters     |
| authentication | Configures TACACS authentication parameters |

**Table 61: AAA TACACS Policy Configuration Commands (continued)**

| Command                    | Description                                                            |
|----------------------------|------------------------------------------------------------------------|
| <code>authorization</code> | Configures TACACS authorization parameters                             |
| <code>no</code>            | Removes this TACACS policy settings or reverts them to default values. |

**Note**

For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see [COMMON COMMANDS](#) on page 640.

**Note**

The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (\_) character. In other words, the name of a device cannot contain an underscore.

*accounting*

Configures the server type and interval at which interim accounting updates are sent to the server. Up to 2 accounting servers can be configured.

This feature tracks user activities on the network, and provides information, such as resources used and the usage time. This information can be used for audit and billing purposes.

TACACS accounting tracks user activity and is useful for security audit purposes.

**Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

**Syntax**

```
accounting [access-method|auth-fail|commands|server|session]
accounting access-method [all|console|ssh|telnet] {(console|ssh|telnet)}
accounting [auth-fail|commands|session]
accounting server [<1-2>|preference]
accounting server preference [authenticated-server-host|authenticated-server-number|
authorized-server-host|authorized-server-number|none]
accounting server <1-2> [host|retry-timeout-factor <50-200>|timeout]
accounting server <1-2> host <IP/HOSTNAME> {secret [0 <SECRET>|2 <SECRET>|
<SECRET>]} {port <1-65535>}
accounting server <1-2> timeout <3-5> {attempts <1-3>}
```

**Parameters**

```
accounting access-method [all|console|ssh|telnet] {(console|ssh|telnet)}
```

|               |                                                                                           |
|---------------|-------------------------------------------------------------------------------------------|
| access-method | Configures TACACS accounting access mode. The options are: console, SSH, Telnet, and all. |
| all           | Configures TACACS accounting for all access modes                                         |
| console       | Configures TACACS accounting for console access only                                      |

|        |                                                     |
|--------|-----------------------------------------------------|
| ssh    | Configures TACACS accounting for SSH access only    |
| telnet | Configures TACACS accounting for Telnet access only |

accounting [auth-fail|commands|session]

|           |                                                                                            |
|-----------|--------------------------------------------------------------------------------------------|
| auth-fail | Enables accounting for authentication fail details. This option is disabled by default.    |
| commands  | Enables accounting of commands executed. This option is disabled by default.               |
| session   | Enables accounting for session start and stop details. This option is disabled by default. |

accounting server preference [authenticated-server-host|authenticated-server-number|authorized-server-host|authorized-server-number|none]

|                             |                                                                                                                                                                                                                      |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| server                      | Configures a TACACS accounting server                                                                                                                                                                                |
| preference                  | Configures the accounting server preference (specifies the method of selecting a server, from the pool, to send the request)                                                                                         |
| authenticated-server-host   | Sets the authentication server as the accounting server. This is the default setting. This parameter indicates the same server is used for authentication and accounting. The server is referred to by its hostname. |
| authenticated-server-number | Sets the authentication server as the accounting server. This parameter indicates the same server is used for authentication and accounting. The server is referred to by its index or number.                       |
| authorized-server-host      | Sets the authorization server as the accounting server. This parameter indicates the same server is used for authorization and accounting. The server is referred to by its hostname.                                |
| authorized-server-number    | Sets the authorized server as the accounting server. This parameter indicates the same server is used for authorization and accounting. The server is referred to by its index number.                               |
| none                        | Indicates the accounting server is independent of the authentication and authorization servers                                                                                                                       |

accounting server <1-2> retry-timeout-factor <50-200>

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| server <1-2>                  | Configures an accounting server. Up to 2 accounting servers can be configured                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| retry-timeout-factor <50-200> | <p>Sets the scaling factor for retry timeouts</p> <ul style="list-style-type: none"> <li>• &lt;50-200&gt; – Specify a value from 50 - 200. The default is 100.</li> </ul> <p>A value of 100 indicates the time gap between two consecutive retries remains the same irrespective of the number of retries.</p> <p>A value lesser than 100 indicates the time gap between two consecutive retries reduces with each successive retry.</p> <p>A value greater than 100 indicates the time gap between two consecutive retries increases with each successive retry.</p> |

accounting server <1-2> host <IP/HOSTNAME> {secret [0 <SECRET>|2 <SECRET>|<SECRET>]} {port <1-65535>}

|                    |                                                                               |
|--------------------|-------------------------------------------------------------------------------|
| server <1-2>       | Configures an accounting server. Up to 2 accounting servers can be configured |
| host <IP/HOSTNAME> | Configures the accounting server's IP address or hostname                     |

|                                           |                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| secret [0 <SECRET>  2 <SECRET>  <SECRET>] | Optional. Configures a common secret key used to authenticate with the accounting server <ul style="list-style-type: none"> <li>0 &lt;SECRET&gt; - Configures a clear text secret key</li> <li>2 &lt;SECRET&gt; - Configures an encrypted secret key</li> <li>&lt;SECRET&gt; - Specify the secret key. This shared secret should not exceed 127 characters.</li> </ul> |
| port <1-65535>                            | Optional. Configures the accounting server port (the port used to connect to the accounting server) <ul style="list-style-type: none"> <li>&lt;1-65535&gt; - Specify the TCP accounting port number from 1 - 65535. The default port is 49.</li> </ul>                                                                                                                 |

accounting server <1-2> timeout <3-5> {attempts <1-3>}

|                |                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| server <1-2>   | Configures an accounting server. Up to 2 accounting servers can be configured                                                                                                                                                                                                                                                                                                                     |
| timeout <3-5>  | Configures the timeout for each request sent to the TACACS accounting server. This is the time allowed to elapse before another request is sent to the TACACS accounting server. If a response is received from the server within this time, no retry is attempted. <ul style="list-style-type: none"> <li>&lt;3-5&gt; - Specify a value from 3 - 5 seconds. The default is 3 seconds.</li> </ul> |
| attempts <1-3> | Optional. Specifies the number of times a transmission request is attempted. This is the maximum number of times a request is sent to the TACACS accounting server before getting discarded. <ul style="list-style-type: none"> <li>&lt;1-3&gt; - Specify a value from 1 - 3. The default is 3.</li> </ul>                                                                                        |

### Examples

```

nx9500-6C8809(config-aaa-tacacs-policy-test)#accounting auth-fail
nx9500-6C8809(config-aaa-tacacs-policy-test)#accounting commands
nx9500-6C8809(config-aaa-tacacs-policy-test)#accounting server preference
authorized-server-number
nx9500-6C8809(config-aaa-tacacs-policy-test)#show context
aaa-tacacs-policy test
 accounting server preference authorized-server-number
 accounting auth-fail
 accounting commands
nx9500-6C8809(config-aaa-tacacs-policy-test)#

```

### Related Commands

|    |                                    |
|----|------------------------------------|
| no | Resets values or disables commands |
|----|------------------------------------|

### authentication

Configures user authentication parameters. Users are allowed or denied access to the network based on the authentication parameters set.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
authentication [access-method|directed-request|server|service]
authentication access-method [all|console|ssh|telnet|web] {(console/ssh/telnet/
web)}
authentication directed-request
authentication server <1-2> [host|retry-timeout-factor|timeout]
authentication server <1-2> host <IP/HOSTNAME> {secret [0 <SECRET>|2 <SECRET>|
<SECRET>]} {port <1-65535>}
authentication server <1-2> retry-timeout-factor <50-200>
authentication server <1-2> timeout <3-60> {attempts <1-10>}
authentication service <SERVICE-NAME> {protocol <AUTHENTICATION-PROTO-NAME>}
```

## Parameters

```
authentication access-method [all|console|ssh|telnet|web] {(console/ssh/telnet/
web)}
```

|               |                                                                                                         |
|---------------|---------------------------------------------------------------------------------------------------------|
| access-method | Configures access modes for TACACS authentication. The options are: console, SSH, Telnet, Web, and all. |
| all           | Authenticates users using all access modes (console, SSH, and Telnet)                                   |
| console       | Authenticates users using console access only                                                           |
| ssh           | Authenticates users using SSH access only                                                               |
| telnet        | Authenticates users using Telnet access only                                                            |
| web           | Authenticates users using Web interface only                                                            |

```
authentication directed-request
```

|                  |                                                                                                                                                                                             |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| directed-request | Enables user to specify TACACS server to use with '@server'. This option is disabled by default.<br><br><b>Note:</b> The specified server should be present in the configured servers list. |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
authentication server <1-2> host <IP/HOSTNAME> {secret [0 <SECRET>|2 <SECRET>|
<SECRET>]} {port <1-65535>}
```

|                                          |                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| server <1-2>                             | Configures a TACACS authentication server. Up to 2 TACACS servers can be configured <ul style="list-style-type: none"><li>&lt;1-2&gt; - Specify the TACACS server index from 1 - 2.</li></ul>                                                                                                                                       |
| host <IP/HOSTNAME>                       | Sets the TACACS server's IP address or hostname                                                                                                                                                                                                                                                                                     |
| secret [0 <SECRET> 2 <SECRET>  <SECRET>] | Configures the secret key used to authenticate with the TACACS server <ul style="list-style-type: none"><li>0 &lt;SECRET&gt; - Configures a clear text secret</li><li>2 &lt;SECRET&gt; - Configures an encrypted secret</li><li>&lt;SECRET&gt; - Specify the secret key. The shared key should not exceed 127 characters.</li></ul> |
| port <1-65535>                           | Optional. Specifies the port used to connect to the TACACS server <ul style="list-style-type: none"><li>&lt;1-65535&gt; - Specify a value for the TCP authentication port from 1 - 65535. The default port is 49.</li></ul>                                                                                                         |

```
authentication server <1-2> retry-timeout-factor <50-200>
```

|                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| server <1-2>                     | Configures a TACACS authentication server. Up to 2 TACACS servers can be configured <ul style="list-style-type: none"> <li>• &lt;1-2&gt; - Specify the TACACS server index from 1 - 2.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                   |
| retry-timeout-factor<br><50-200> | Configures timeout scaling between two consecutive TACACS authentication retries <ul style="list-style-type: none"> <li>• &lt;50-200&gt; - Specify the scaling factor from 50 - 200. The default is 100.</li> </ul> <p>A value of 100 indicates the interval between consecutive retries remains the same irrespective of the number of retries.</p> <p>A value lesser than 100 indicates the interval between consecutive retries reduces with each successive retry.</p> <p>A value greater than 100 indicates the interval between consecutive retries increases with each successive retry.</p> |

```
authentication server <1-2> timeout <3-60> {attempts <1-10>}
```

|                    |                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| server <1-2>       | Configures a TACACS authentication server. Up to 2 TACACS servers can be configured <ul style="list-style-type: none"> <li>• &lt;1-2&gt; - Specify the TACACS server index from 1- 2.</li> </ul>                                                                                                                                                                                                   |
| timeout<br><3-60>  | Configures the timeout, in seconds, for each request sent to the TACACS server. This is the time allowed to elapse before another request is sent to the TACACS server. If a response is received from the TACACS server within this time, no retry is attempted. <ul style="list-style-type: none"> <li>• &lt;3-60&gt; - Specify a value from 3- 60 seconds. The default is 3 seconds.</li> </ul> |
| attempts<br><1-10> | Optional. Indicates the number of retry attempts to make before giving up <ul style="list-style-type: none"> <li>• &lt;1-10&gt; - Specify a value from 1 -10. The default is 3.</li> </ul>                                                                                                                                                                                                         |

```
authentication service <SERVICE-NAME> {protocol <AUTHENTICATION-PROTO-NAME>}
```

|                                      |                                                                                                                                  |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| service <SERVICE-NAME>               | Configures the TACACS authentication service name                                                                                |
| protocol <AUTHENTICATION-PROTO-NAME> | Optional. Specify the authentication protocol used with this TACACS policy<br><b>Note:</b> A maximum of five entries is allowed. |

## Examples

```
nx9500-6C8809(config-aaa-tacacs-policy-test)#authentication directed-request
nx9500-6C8809(config-aaa-tacacs-policy-test)#show context
aaa-tacacs-policy test
 authentication directed-request
 accounting server preference authorized-server-number
 accounting auth-fail
 accounting commands
nx9500-6C8809(config-aaa-tacacs-policy-test)#
```

## Related Commands

|    |                                    |
|----|------------------------------------|
| no | Resets values or disables commands |
|----|------------------------------------|

## authorization

Configures AAA TACACS authorization parameters

This feature allows network administrators to limit user accessibility and configure varying levels of accessibility for different users.



## Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
authorization [access-method|allow-privileged-commands|server]
authorization access-method [all|console|telnet|ssh] {(console|ssh|telnet)}
authorization server [<1-2>|preference]
authorization server <1-2> [host|retry-timeout-factor|timeout]
authorizationserver <1-2> host <IP/HOSTNAME> {secret [0 <SECRET>|2 <SECRET>|
<SECRET>]} {port <1-65535>}
authorization server <1-2> retry-timeout-factor <50-200>
authorization server <1-2> timeout <3-5> {attempts <1-3>}
authorization server preference [authenticated-server-host|authenticated-server-number|
none]
```

## Parameters

```
authorization access-method [all|console|telnet|ssh] {(console|ssh|telnet)}
```

|                      |                                                                            |
|----------------------|----------------------------------------------------------------------------|
| access-method        | Configures the access method for command authorization                     |
| all                  | Authorizes commands from all access methods                                |
| console              | Authorizes commands from the console only                                  |
| telnet               | Authorizes commands from Telnet only                                       |
| ssh                  | Authorizes commands from SSH only                                          |
| {console ssh telnet} | Optional. Configures more than one access method for command authorization |

```
authorization allow-privileged-commands
```

|                           |                                                                                                         |
|---------------------------|---------------------------------------------------------------------------------------------------------|
| allow-privileged-commands | Allows privileged commands execution without command authorization. This option is disabled by default. |
|---------------------------|---------------------------------------------------------------------------------------------------------|

```
authorization server <1-2> host <IP/HOSTNAME> {secret [0 <SECRET>|2 <SECRET>|
<SECRET>]} {port <1-65535>}
```

|                                         |                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| server <1-2>                            | Configures a TACACS authorization server. Up to 2 TACACS servers can be configured <ul style="list-style-type: none"><li>• &lt;1-2&gt; - Specify the TACACS server index from 1 - 2.</li></ul>                                                                                                                                               |
| host <IP/HOSTNAME>                      | Sets the TACACS server's IP address or hostname                                                                                                                                                                                                                                                                                              |
| secret [0 <SECRET> 2 <SECRET> <SECRET>] | Optional. Configures the secret used to authorize with the TACACS server <ul style="list-style-type: none"><li>• 0 &lt;SECRET&gt; - Configures a clear text secret</li><li>• 2 &lt;SECRET&gt; - Configures an encrypted secret</li><li>• &lt;SECRET&gt; - Specify the secret key. The shared key should not exceed 127 characters.</li></ul> |
| port <1-65535>                          | Optional. Specifies the port used to connect to the TACACS server <ul style="list-style-type: none"><li>• &lt;1-65535&gt; - Specify a value for the TCP authorization port from 1 - 65535. The default port is 49.</li></ul>                                                                                                                 |

```
authorization server <1-2> retry-timeout-factor <50-200>
```

|                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| server <1-2>                     | Configures a TACACS authorization server. Up to 2 TACACS servers can be configured <ul style="list-style-type: none"> <li>• &lt;1-2&gt; – Specify the TACACS server index from 1 - 2.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                       |
| retry-timeout-factor<br><50-200> | Configures the scaling of timeouts between consecutive TACACS authorization retries <ul style="list-style-type: none"> <li>• &lt;50-200&gt; – Specify the scaling factor from 50 - 200. The default is 100.</li> </ul> <p>A value of 100 indicates the interval between consecutive retries remains the same irrespective of the number of retries.</p> <p>A value lesser than 100 indicates the interval between consecutive retries reduces with each successive retry.</p> <p>A value greater than 100 indicates the interval between consecutive retries increases with each successive retry.</p> |

```
authorization server <1-2> timeout <3-5> {attempts <1-3>}
```

|                |                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| server <1-2>   | Configures a TACACS authorization server. Up to 2 TACACS servers can be configured <ul style="list-style-type: none"> <li>• &lt;1-2&gt; – Specify the TACACS server's index from 1- 2.</li> </ul>                                                                                                                                                                                                 |
| timeout <3-5>  | Configures the timeout, in seconds, for each request sent to the TACACS server. This is the time allowed to elapse before another request is sent to the TACACS server. If a response is received from the TACACS server within this time, no retry is attempted. <ul style="list-style-type: none"> <li>• &lt;3-5&gt; – Specify a value from 3 - 5 seconds. The default is 3 seconds.</li> </ul> |
| attempts <1-3> | Optional. Indicates the number of retry attempts to make before giving up <ul style="list-style-type: none"> <li>• &lt;1-3&gt; – Specify a value from 1 - 3. The default is 3.</li> </ul>                                                                                                                                                                                                         |

```
authorization server preference [authenticated-server-host|authenticated-server-number|none]
```

|                             |                                                                                                                                                                                                        |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| preference                  | Configures the authorization server preference                                                                                                                                                         |
| authenticated-server-host   | Sets the authentication server as the authorization server<br>This parameter indicates the same server is used for authentication and authorization. The server is referred to by its hostname.        |
| authenticated-server-number | Sets the authentication server as the authorization server<br>This parameter indicates the same server is used for authentication and authorization. The server is referred to by its index or number. |
| none                        | Indicates the authorization server is independent of the authentication server                                                                                                                         |

## Examples

```
nx9500-6C8809(config-aaa-tacacs-policy-test)#authorization allow-privileged-commands
nx9500-6C8809(config-aaa-tacacs-policy-test)#show context
aaa-tacacs-policy test
 authentication directed-request
 accounting server preference authorized-server-number
 authorization allow-privileged-commands
 accounting auth-fail
 accounting commands
nx9500-6C8809(config-aaa-tacacs-policy-test)#
```

## Related Commands

|    |                                    |
|----|------------------------------------|
| no | Resets values or disables commands |
|----|------------------------------------|

no

Removes this AAA TACACS policy settings or reverts to default values

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
no [accounting|authentication|authorization]
```

#### Parameters

```
no <PARAMETERS>
```

no <PARAMETERS> Removes this AAA TACACS policy settings or reverts to default values, based on the parameters passed

#### Examples

The following example shows the AAA-TACACS policy 'test' settings before the 'no' commands are executed:

```
<exsw1>(config-aaa-tacacs-policy-test)#show context
aaa-tacacs-policy test
 authentication directed-request
 accounting server preference authorized-server-number
 authorization allow-privileged-commands
 accounting auth-fail
 accounting commands
<exsw1>(config-aaa-tacacs-policy-test)#
<exsw1>(config-aaa-tacacs-policy-test)#no authentication directed-request
<exsw1>(config-aaa-tacacs-policy-test)#no accounting auth-fail
<exsw1>(config-aaa-tacacs-policy-test)#no authorization allow-privileged-commands
```

The following example shows the AAA-TACACS policy 'test' settings after the 'no' commands are executed:

```
<exsw1>(config-aaa-tacacs-policy-test)#show context
aaa-tacacs-policy test
 accounting server preference authorized-server-number
 accounting commands
<exsw1>(config-aaa-tacacs-policy-test)#
```

# MESHPOINT

## MESHPOINT

---

This chapter summarizes the Meshpoint commands in the CLI command structure.

Meshpoints are detector radios that monitor their coverage areas for potential failed peers or coverage area holes requiring transmission adjustments for coverage compensation.

This chapter is organized as follows:

- [meshpoint config instance](#)
- [meshpoint-qos-policy-config-instance](#)
- [meshpoint-device-config-instance](#) on page 1787

### meshpoint-config-instance

MCX (MeshConnex) is a mesh networking technology that is comparable to the 802.11s mesh networking specification. MeshConnex meshing uses a hybrid proactive/on-demand path selection protocol, similar to AODV (Ad-hoc On Demand Distance Vector) routing protocols. This allows it to form efficient paths using multiple attachment points to a distribution WAN, or form purely ad-hoc peer-to-peer mesh networks in the absence of a WAN. Each device in the MeshConnex mesh proactively manages its own path to the distribution WAN, but can also form peer-to-peer paths on demand to improve forwarding efficiency.

MeshConnex is not compatible with MiNT Based meshing, though the two technologies can be enabled simultaneously in certain circumstances.

MeshConnex is designed for large-scale, high-mobility outdoor mesh deployments. MeshConnex continually gathers data from beacons and transmission attempts to estimate the efficiency and throughput of each MP-to-MP link. MeshConnex uses this data to dynamically form and continually maintain paths for forwarding network frames.

In MeshConnex systems, a MP (mesh point) is a virtual mesh networking instance on a device, similar to a WLAN AP. On each device, up to 4 MPs can be created and 2 can be created per radio. MPs can be configured to use one or both radios in the device. If the MP is configured to use both radios, the path selection protocols continuously selects the best radio to reach each destination. Each MP participates in a single Mesh Network, defined by the MeshID. The MeshID is typically a descriptive network name, similar to the SSID of a WLAN. All MPs configured to use the same MeshID attempt to form a mesh and interoperate. The MeshID allows overlapping mesh networks to discriminate and disregard MPs belonging to different networks.

Use the (config) instance to configure meshpoint related configuration commands. To navigate to the meshpoint instance, use the following command:

```
<DEVICE>(config)#meshpoint <MESHPOINT-NAME>
nx9500-6C8809(config)#meshpoint test
nx9500-6C8809(config-meshpoint-test)#?
Mesh Point Mode commands:
```

```

allowed-vlans Set the allowed VLANs
beacon-format The beacon format of this meshpoint
control-vlan VLAN for meshpoint control traffic
data-rates Specify the 802.11 rates to be supported on this meshpoint
description Configure a description of the usage of this meshpoint
force Force suboptimal paths
meshid Configure the Service Set Identifier for this meshpoint
neighbor Configure neighbor specific parameters
no Negate a command or set its defaults
root Set this meshpoint as root
security-mode The security mode of this meshpoint
shutdown Shutdown this meshpoint
use Set setting to use
wpa2 Modify ccmp wpa2 related parameters

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

```

nx9500-6C8809(config-meshpoint-test)#

The following table summarizes meshpoint configuration commands.

*Table: Meshpoint-Config commands*

| Command                                                       | Description                                                             |
|---------------------------------------------------------------|-------------------------------------------------------------------------|
| <a href="#">allowed-vlans (meshpoint-config)</a> on page 1762 | Configures VLANs allowed on the meshpoint                               |
| <a href="#">beacon-format (meshpoint-config)</a> on page 1763 | Configures the beacon format for the meshpoint AP                       |
| <a href="#">control-vlan (meshpoint-config)</a> on page 1764  | Configures the VLAN where meshpoint control traffic traverses           |
| <a href="#">data-rates (meshpoint-config)</a> on page 1765    | Configures the data rates supported per frequency band                  |
| <a href="#">description (meshpoint-config)</a> on page 1768   | Configures a human friendly description for this meshpoint              |
| <a href="#">force (meshpoint-config)</a> on page 1769         | Forces formation of sub-optimal paths through the meshpoint's root node |
| <a href="#">meshid (meshpoint-config)</a> on page 1769        | Configures a unique ID for this meshpoint                               |
| <a href="#">neighbor (meshpoint-config)</a> on page 1770      | Configures the neighbor inactivity time out for this meshpoint          |
| <a href="#">root (meshpoint-config)</a> on page 1771          | Configures a meshpoint as the root meshpoint                            |
| <a href="#">security-mode (meshpoint-config)</a> on page 1773 | Configures the security mode on the meshpoint.                          |
| <a href="#">service (meshpoint-config)</a> on page 1774       | Allows only 802.11n capable neighbors to create a mesh connection       |
| <a href="#">shutdown (meshpoint-config)</a> on page 1775      | Shuts down the meshpoint                                                |
| <a href="#">use (meshpoint-config)</a> on page 1775           | Associates a QoS policy with this meshpoint                             |

| Command                                           | Description                                |
|---------------------------------------------------|--------------------------------------------|
| <code>wpa2 (meshpoint-config)</code> on page 1776 | Configures WPA2 encryption settings        |
| <code>no (meshpoint-config)</code> on page 1780   | Removes or reverts this Meshpoint settings |



#### Note

For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see [COMMON COMMANDS](#).



#### Note

The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (\_) character. In other words, the name of a device cannot contain an underscore.

### *allowed-vlans (meshpoint-config)*

Defines VLANs allowed on the mesh network. A VLAN must be added to the allowed VLANs list for data to be allowed across the mesh network. Use this command to add and remove VLANs from the list of allowed VLANs.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
allowed-vlans [<VLAN-ID> | add <VLAN-ID> | remove <VLAN-ID>]
```

#### Parameters

```
allowed-vlans [<VLAN-ID> | add <VLAN-ID> | remove <VLAN-ID>]
```

|                  |                                                                                                                                                                                                                                                                                                                    |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| allowed-vlans    | Defines VLANs allowed access on the mesh network                                                                                                                                                                                                                                                                   |
| <VLAN-ID>        | Specifies the VLAN ID or the range of IDs to be managed.<br>A single VLAN or multiple VLANs can be added to the list of allowed VLANs. When adding multiple VLANs, specify the range (for example, 10-20, 25, 30-35). Use this command to create a VLAN list on a new meshpoint.                                   |
| add <VLAN-ID>    | Adds a single VLAN or a range of VLANs to the list of allowed VLANs. To specify a range of VLANs, specify the first and last VLAN ID in the range separated by a hyphen (for example, 1-10). <ul style="list-style-type: none"> <li>• &lt;VLAN-ID&gt; - Specify the VLAN ID or the range of IDs to add.</li> </ul> |
| remove <VLAN-ID> | Removes a single VLAN or a range of VLANs from the list of allowed VLANs. <ul style="list-style-type: none"> <li>• &lt;VLAN-ID&gt; - Specify the VLAN ID or the range of IDs to remove.</li> </ul>                                                                                                                 |

## Examples

```
nx9500-6C8809(config-meshpoint-test)#allowed-vlans 1
nx9500-6C8809(config-meshpoint-test)#allowed-vlans add 10-23
nx9500-6C8809(config-meshpoint-test)#allowed-vlans remove 17
nx9500-6C8809(config-meshpoint-test)#show context
meshpoint test
 meshid test
 beacon-format mesh-point
 control-vlan 1
 allowed-vlans 1,10-16,18-23
 security-mode none
 no root
nx9500-6C8809(config-meshpoint-test)#
```

## Related Commands

|                                                 |                                                             |
|-------------------------------------------------|-------------------------------------------------------------|
| <code>no (meshpoint-config)</code> on page 1780 | Clears the list of VLANs allowed access to the mesh network |
|-------------------------------------------------|-------------------------------------------------------------|

### *beacon-format (meshpoint-config)*

Configures the beacon transmission format for this meshpoint. Beacons are transmitted periodically to advertise that a wireless network is available. It contains all the required information for a device to connect to the network.

The beacon format advertises how a mesh-capable access point acts. APs can act either as an access point or a meshpoint.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
beacon-format [access-point|mesh-point]
```

## Parameters

```
beacon-format [access-point|mesh-point]
```

|               |                                                                   |
|---------------|-------------------------------------------------------------------|
| beacon-format | Configures how a mesh capable access point acts in a mesh network |
| access-point  | Uses access point style beacons                                   |
| mesh-point    | Uses meshpoint style beacons (this is the default setting)        |

## Examples

```
nx9500-6C8809(config-meshpoint-test)#beacon-format access-point
nx9500-6C8809(config-meshpoint-test)#show context
meshpoint test
 meshid test
 beacon-format access-point
 control-vlan 1
 allowed-vlans 1,10-16,18-23
 security-mode none
```

```

no root
nx9500-6C8809(config-meshpoint-test)#
nx9500-6C8809(config-meshpoint-test)#no beacon-format
nx9500-6C8809(config-meshpoint-test)#show context
meshpoint test
meshid test
beacon-format mesh-point
control-vlan 1
allowed-vlans 1,10-16,18-23
security-mode none
no root
nx9500-6C8809(config-meshpoint-test)#

```

## Related Commands

`no (meshpoint-config)` on page 1780 Resets the beacon format for this meshpoint to its default (mesh-point)

### *control-vlan (meshpoint-config)*

Configures a VLAN as the dedicated control VLAN for this meshpoint

Mesh management traffic can be sent over a dedicated VLAN. This dedicated VLAN is known as the control VLAN, and should be configured in the backhaul port of all the access points configured as meshpoint roots. Once configured, the control VLAN carries the mesh point's control traffic.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
control-vlan [<1-4094>|<VLAN-ALIAS-NAME>]
```

### Parameters

```
control-vlan [<1-4094>|<VLAN-ALIAS-NAME>]
```

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| control-vlan                 | Configures a VLAN as a dedicated carrier of mesh management traffic                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| [<1-4094> <VLAN-ALIAS-NAME>] | <p>Configures the control VLAN</p> <ul style="list-style-type: none"> <li>• &lt;1-4094&gt; - Specify the control VLAN from 1 - 4094. The default is VLAN 1.</li> <li>• &lt;VLAN-ALIAS-NAME&gt; - Uses a vlan-alias to specify the control vlan. If using a vlan-alias, ensure that it is existing and configured.</li> </ul> <p>If VLAN 1 is configured as the control VLAN, ensure that the VLAN is configured in the wired port of all access points belonging to same meshpoint.</p> <p><b>Note:</b> Control VLAN need not necessarily be added in the allowed VLAN list.</p> |

### Examples

```

nx9500-6C8809(config-meshpoint-test)#control-vlan 25
nx9500-6C8809(config-meshpoint-test)#show context
meshpoint test
meshid test

```



```

beacon-format mesh-point
control-vlan 25
allowed-vlans 1,10-16,18-23
security-mode none
no root
nx9500-6C8809(config-meshpoint-test)#

```

### Related Commands

`no (meshpoint-config)` on page 1780 Resets the control VLAN for this meshpoint to its default value of VLAN 1

### *data-rates (meshpoint-config)*

Configures individual data rates for the 2.4 GHz and 5.0 GHz frequency bands. In Mesh network, a mesh point is a virtual mesh networking instance on a device, similar to a WLAN AP. On each device, up to 4 mesh points can be created and 2 can be created per radio. Each mesh point radio can have carefully administrated radio rates specific to the 2.4 or 5 GHz band. Use this command to configure these radio rates.



#### Note

Ensure that the basic data rates configured on a meshpoint's root and non-root access points is the same.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```

data-rates [2.4GHz|5GHz]
data-rates 2.4GHz [b-only|bg|bgn|default|g-only|gn]
data-rates 2.4GHz custom (1|11|12|18|2|24|36|48|5.5|54|6|9|basic-1|basic-11|
basic-12|basic-18|basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|basic-6|basic-9|
mcs0-15|mcs0-7|mcs8-15|basic-mcs0-7)
data-rates 5GHz [a-only|an|default]
data-rates 5GHz custom (12|18|24|36|48|54|6|9|basic-1|basic-11|basic-12|basic-18|
basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|basic-6|basic-9|mcs0-15|mcs0-7|
mcs8-15|
basic-mcs0-7)

```

### Parameters

```
data-rates 2.4GHz [b-only|bg|bgn|default|g-only|gn]
```

|                   |                                                                                             |
|-------------------|---------------------------------------------------------------------------------------------|
| data-rates 2.4GHz | Configures preset data rates for the 2.4 GHz frequency.                                     |
| b-only            | Configures data rate for the meshpoint using 802.11b only rates.                            |
| bg                | Configures data rate for the meshpoint using 802.11b and 802.11g rates.                     |
| default           | Configures data rate for the meshpoint at a pre-configured default rate for this frequency. |

|        |                                                                         |
|--------|-------------------------------------------------------------------------|
| g-only | Configures data rate for the meshpoint using 802.11g only rates.        |
| gn     | Configures data rate for the meshpoint using 802.11g and 802.11n rates. |

```
data-rates 2.4GHz custom (1|11|12|18|2|24|36|48|5.5|54|6|9|basic-1|basic-11|
basic-12|basic-18|basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|basic-6|basic-9|
mcs0-15|mcs0-7|mcs8-15|basic-mcs0-7)
```

|                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| data-rates 2.4GHz                                                                                                                                                                      | <p>Configures the preset data rates for the 2.4 GHz frequency</p> <p>Define both minimum <b>Basic</b> and optimal <b>Supported</b> rates as required for the 802.11b rates, 802.11g rates and 802.11n rates supported by the 2.4 GHz band. These are the rates wireless client traffic is supported within this mesh point.</p> <p>These are the rates wireless client traffic is supported within this mesh point. If supporting 802.11n, select a supported MCS index. Set a MCS (Modulation and Coding Scheme) in respect to the radio's channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of 8 data rates, bonded channels, multiple spatial streams, different guard intervals and modulation types.</p> <p>Meshpoints can communicate as long as they support the same basic MCS (as well as non-802.11n basic rates). The selected rates apply to associated client traffic within this mesh point only.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| custom (1 11 12 18 2 24 36 48 5.5 54 6 9 basic-1 basic-11 basic-12 basic-18 basic-2 basic-24 basic-36 basic-48 basic-5.5 basic-54 basic-6 basic-9 mcs0-15 mcs0-7 mcs8-15 basic-mcs0-7) | <p>Configures custom rates</p> <ul style="list-style-type: none"> <li>• 1 – Configures the available rate at 1 Mbps</li> <li>• 2 – Configures the available rate at 2 Mbps</li> <li>• 5.5 – Configures the available rate at 5.5 Mbps</li> <li>• 6 – Configures the available rate at 6 Mbps</li> <li>• 9 – Configures the available rate at 9 Mbps</li> <li>• 11 – Configures the available rate at 11 Mbps</li> <li>• 12 – Configures the available rate at 12 Mbps</li> <li>• 18 – Configures the available rate at 18 Mbps</li> <li>• 24 – Configures the available rate at 24 Mbps</li> <li>• 36 – Configures the available rate at 36 Mbps</li> <li>• 48 – Configures the available rate at 48 Mbps</li> <li>• 54 – Configures the available rate at 54 Mbps</li> <li>• basic-1 – Configures the available rate at a basic rate of 1 Mbps</li> <li>• basic-2 – Configures the available rate at a basic rate of 2 Mbps</li> <li>• basic-5.5 – Configures the available rate at a basic rate of 5.5 Mbps</li> <li>• basic-6 – Configures the available rate at a basic rate of 6 Mbps</li> <li>• basic-9 – Configures the available rate at a basic rate of 9 Mbps</li> <li>• basic-11 – Configures the available rate at a basic rate of 11 Mbps</li> <li>• basic-12 – Configures the available rate at a basic rate of 12 Mbps</li> <li>• basic-18 – Configures the available rate at a basic rate of 18 Mbps</li> <li>• basic-24 – Configures the available rate at a basic rate of 24 Mbps</li> <li>• basic-36 – Configures the available rate at a basic rate of 36 Mbps</li> <li>• basic-48 – Configures the available rate at a basic rate of 48 Mbps</li> <li>• basic-54 – Configures the available rate at a basic rate of 54 Mbps</li> <li>• basic-mcs0-7 – Configures the MCS index range of 0 - 7 for basic rate</li> <li>• mcs0-7 – Configures the MCS index range of 0-7 as the data rate</li> <li>• mcs0-15 – Configures the MCS index range of 0-15 as the data rate</li> <li>• msc8-15 – Configures the MCS index range of 8-15 as the data rate</li> </ul> <p>Multiple choices can be made from the above list of rates</p> |

```
data-rates 5GHz [a-only|an|default]
```

|                 |                                                                                                |
|-----------------|------------------------------------------------------------------------------------------------|
| data-rates 5GHz | Configures the preset data rates for the 5.0 GHz frequency                                     |
| a-only          | Configures the data rate for the meshpoint using 802.11a only rates                            |
| bn              | Configures the data rate for the meshpoint using 802.11a and 802.11n rates                     |
| default         | Configures the data rate for the meshpoint at a pre-configured default rate for this frequency |
| g-only          | Configures the data rate for the meshpoint using 802.11g only rates                            |
| gn              | Configures the data rate for the meshpoint using 802.11g and 802.11n rates                     |

```
data-rates 5GHz custom (12|18|24|36|48|54|6|9|basic-1|basic-11|basic-12|basic-18|
basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|basic-6|basic-9|mcs0-15|mcs0-7|
mcs8-15|
basic-mcs0-7)
```

|                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| data-rates 5GHz                                                                                                                                                                                     | <p>Configures the preset data rates for the 5.0 GHz frequency</p> <p>Define both minimum <b>Basic</b> and optimal <b>Supported</b> rates as required for 802.11a and 802.11n rates supported by the 5.0 GHz radio band. These are the rates wireless client traffic is supported within this mesh point.</p> <p>If supporting 802.11n, select a supported MCS index. Set a MCS in respect to the radio's channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of 8 data rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Mesh points can communicate as long as they support the same basic MCS (as well as non-802.11n basic rates). The selected rates apply to associated client traffic within this mesh point only.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <pre>custom (12 18 24  36 48 54  6 9  basic-1 basic-11  basic-12 basic-18  basic-2  basic-24  basic-36 basic-48  basic-5.5  basic-54 basic-6  basic-9 mcs0-15  mcs0-7  mcs8-15  basic-mcs0-7)</pre> | <p>Configures custom rates</p> <ul style="list-style-type: none"> <li>• 6 – Configures the available rate at 6 Mbps</li> <li>• 9 – Configures the available rate at 9 Mbps</li> <li>• 12 – Configures the available rate at 12 Mbps</li> <li>• 18 – Configures the available rate at 18 Mbps</li> <li>• 24 – Configures the available rate at 24 Mbps</li> <li>• 36 – Configures the available rate at 36 Mbps</li> <li>• 48 – Configures the available rate at 48 Mbps</li> <li>• 54 – Configures the available rate at 54 Mbps</li> <li>• basic-1 – Configures the available rate at a basic rate of 1 Mbps</li> <li>• basic-2 – Configures the available rate at a basic rate of 2 Mbps</li> <li>• basic-5.5 – Configures the available rate at a basic rate of 5.5 Mbps</li> <li>• basic-6 – Configures the available rate at a basic rate of 6 Mbps</li> <li>• basic-9 – Configures the available rate at a basic rate of 9 Mbps</li> <li>• basic-11 – Configures the available rate at a basic rate of 11 Mbps</li> <li>• basic-12 – Configures the available rate at a basic rate of 12 Mbps</li> <li>• basic-18 – Configures the available rate at a basic rate of 18 Mbps</li> <li>• basic-24 – Configures the available rate at a basic rate of 24 Mbps</li> <li>• basic-36 – Configures the available rate at a basic rate of 36 Mbps</li> <li>• basic-48 – Configures the available rate at a basic rate of 48 Mbps</li> <li>• basic-54 – Configures the available rate at a basic rate of 54 Mbps</li> <li>• basic-mcs0-7 – Configures the MCS index range of 0-7 for basic rate</li> <li>• mcs0-7 – Configures the MCS index range of 0-7 as the data rate</li> <li>• mcs0-15 – Configures the MCS index range of 0-15 as the data rate</li> <li>• mcs8-15 – Configures the MCS index range of 8-15 as the data rate</li> </ul> <p>Multiple choices can be made from the above list of rates.</p> |

## Examples

```
nx9500-6C8809(config-meshpoint-test)#data-rates 2.4GHz bgn
nx9500-6C8809(config-meshpoint-test)#data-rates 5GHz an
nx9500-6C8809(config-meshpoint-test)#show context
meshpoint test
 meshid test
 beacon-format mesh-point
 control-vlan 25
 allowed-vlans 1,10-16,18-23
 data-rates 2.4GHz bgn
 data-rates 5GHz an
 security-mode none
 no root
nx9500-6C8809(config-meshpoint-test)#
```

## Related Commands

|                                                 |                                                              |
|-------------------------------------------------|--------------------------------------------------------------|
| <code>no (meshpoint-config)</code> on page 1780 | Resets data rates for each frequency band for this meshpoint |
|-------------------------------------------------|--------------------------------------------------------------|

### *description (meshpoint-config)*

Configures a brief description for this meshpoint

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
description <DESCRIPTION>
```

## Parameters

```
description <DESCRIPTION>
```

|               |                                                                                                                                                      |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| description   | Configures a description for this meshpoint                                                                                                          |
| <DESCRIPTION> | The text describing this meshpoint. Enter a 64 character maximum description about the mesh point that uniquely identifies it from other meshpoints. |

## Examples

```
nx9500-6C8809(config-meshpoint-test)#description "This is an example of a meshpoint
description"
nx9500-6C8809(config-meshpoint-test)#show context
meshpoint test
 description "This is an example of a meshpoint description."
 meshid test
 beacon-format mesh-point
 control-vlan 25
 allowed-vlans 1,10-16,18-23
 data-rates 2.4GHz bgn
 data-rates 5GHz an
 security-mode none
 no root
nx9500-6C8809(config-meshpoint-test)#
```

## Related Commands

`no (meshpoint-config)` on page 1780 Removes the human friendly description provided for this meshpoint

### *force (meshpoint-config)*

Forces formation of sub-optimal paths through the meshpoint's root node. As per legacy behavior, non-root devices under the same root, communicated by forming direct paths through the network. This option allows non-root devices, within the meshpoint, to communicate by forming paths through the root node.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
force [peer-paths-through-root|peer-paths-with-root]
```

#### Parameters

```
force [peer-paths-through-root|peer-paths-with-root]
```

|                         |                                                                                                                                                                                    |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| force                   | Forces formation of sub-optimal paths through the meshpoint root node.                                                                                                             |
| peer-paths-through-root | Forces non-root devices to communicate by forming sub-optimal paths through the root node. This option is disabled by default.                                                     |
| peer-paths-with-root    | Forces non-root devices to communicate by forming sub-optimal paths with the root node. Does not allow formation of ad-hoc peer-to-peer paths. This option is disabled by default. |

#### Examples

```
nx9500-6C8809(config-meshpoint-test)#force peer-paths-through-root
nx9500-6C8809(config-meshpoint-test)#show context
meshpoint test
 meshid test
 beacon-format mesh-point
 control-vlan 25
 security-mode none
 no root
 force peer-paths-through-root
nx9500-6C8809(config-meshpoint-test)#
```

## Related Commands

`no (meshpoint-config)` on page 1780 Disables formation of sub-optimal paths

### *meshid (meshpoint-config)*

Configures a unique SSID (Service Set Identifier) for this meshpoint. This ID is used to uniquely identify this meshpoint.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
meshid <MESH-SSID>
```

### Parameters

```
meshid <MESH-SSID>
```

|             |                                                                                   |
|-------------|-----------------------------------------------------------------------------------|
| meshid      | Configures a unique SSID for the meshpoint                                        |
| <MESH-SSID> | The unique SSID configured for this meshpoint                                     |
|             | <b>Note:</b> The mesh SSID is case sensitive and should not exceed 32 characters. |

### Examples

```
nx9500-6C8809(config-meshpoint-test)#meshid TestingMeshPoint
nx9500-6C8809(config-meshpoint-test)#show context
meshpoint test
description "This is an example of a meshpoint description"
meshid TestingMeshPoint
beacon-format mesh-point
control-vlan 1
allowed-vlans 1,10-16,18-23
data-rates 2.4GHz bgn
data-rates 5GHz an
security-mode none
no root
nx9500-6C8809(config-meshpoint-test)#
```

### Related Commands

|                                                    |                                                |
|----------------------------------------------------|------------------------------------------------|
| <a href="#">no (meshpoint-config)</a> on page 1780 | Removes the SSID configured for this meshpoint |
|----------------------------------------------------|------------------------------------------------|

### *neighbor (meshpoint-config)*

This command configures the inactivity time out value for neighboring devices. If a frame is not received from the neighbor device for the configured time, then client resources are removed.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
neighbor inactivity-timeout <60-86400>
```

## Parameters

neighbor inactivity-timeout <60-86400>

|                                        |                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| neighbor inactivity-timeout <60-86400> | Configures the neighbor inactivity timeout in seconds. This represents the allowed interval between frames received from a neighbor before their client privileges are revoked. <ul style="list-style-type: none"><li>• &lt;60-86400&gt; – Specify a value from 60 - 86400 seconds. The default is 120 seconds.</li></ul> |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-meshpoint-test)#neighbor inactivity-timeout 300
nx9500-6C8809(config-meshpoint-test)#show context
meshpoint test
 description "This is an example of a meshpoint description"
 meshid TestingMeshPoint
 beacon-format mesh-point
 control-vlan 25
 allowed-vlans 1,10-16,18-23
 neighbor inactivity-timeout 300
 data-rates 2.4GHz bgn
 data-rates 5GHz an
 security-mode none
 no root
nx9500-6C8809(config-meshpoint-test)#
```

## Related Commands

|                                                    |                                                                              |
|----------------------------------------------------|------------------------------------------------------------------------------|
| <a href="#">no (meshpoint-config)</a> on page 1780 | Removes the configured neighbor inactivity time out value for this meshpoint |
|----------------------------------------------------|------------------------------------------------------------------------------|

### *root (meshpoint-config)*

Configures this meshpoint as the root meshpoint. Root meshpoints are generally tied to an Ethernet backhaul for wired connectivity. By default this option is disabled.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

root

## Parameters

None

## Examples

There are two ways of configuring root access points within a meshpoint.

- 1 First method:
  - Configure two meshpoints, having the same meshid, one with the *root* option enabled and the other configured as *no root*

- Apply the root meshpoint to the root access point and the no-root meshpoint to the non-root access points.

The following examples show the configuration of a meshpoint for the root access point:

```

nx9500-6C8809(config)#meshpoint root
nx9500-6C8809(config-meshpoint-root)#
nx9500-6C8809(config-meshpoint-root)#meshid test
nx9500-6C8809(config-meshpoint-root)#root
nx9500-6C8809(config-meshpoint-root)#security-mode eap
nx9500-6C8809(config-meshpoint-root)#commit
nx9500-6C8809(config-meshpoint-root)#show context
meshpoint root
 meshid test
 beacon-format mesh-point
 control-vlan 1
 security-mode eap
 root
nx9500-6C8809(config-meshpoint-root)#

```

The following examples show the configuration of a meshpoint for non-root access points:

```

nx9500-6C8809(config)#meshpoint no-root
nx9500-6C8809(config-meshpoint-no-root)#
nx9500-6C8809(config-meshpoint-no-root)#meshid test
nx9500-6C8809(config-meshpoint-no-root)#security-mode eap
nx9500-6C8809(config-meshpoint-no-root)#show context
meshpoint no-root
 meshid test
 beacon-format mesh-point
 control-vlan 1
 security-mode eap
 no root
nx9500-6C8809(config-meshpoint-no-root)#

```

## 2 Second method:

- Configure a no-root meshpoint and apply to all access points in the meshpoint.
- Log into the **meshpoint-device > no-root** configuration mode of the root access point and enable root.

```

nx9500-6C8809(config-meshpoint-no-root)#show context
meshpoint no-root
 meshid test
 beacon-format mesh-point
 control-vlan 1
 security-mode eap
 no root
nx9500-6C8809(config-meshpoint-no-root)#
nx9500-6C8809(config)#ap8lxx B4-C7-99-71-17-28
nx9500-6C8809(config-device-B4-C7-99-71-17-28)#meshpoint-device no-root
nx9500-6C8809(config-device-B4-C7-99-71-17-28-meshpoint-no-root)#
nx9500-6C8809(config-device-B4-C7-99-71-17-28-meshpoint-no-root)#show context
meshpoint no-root
 meshid test
 beacon-format mesh-point
 control-vlan 1
 security-mode eap
 no rootnx9500-6C8809(config-device-B4-C7-99-71-17-28-meshpoint-no-root)#
nx9500-6C8809(config-device-B4-C7-99-71-17-28-meshpoint-no-root)#root
nx9500-6C8809(config-device-B4-C7-99-71-17-28-meshpoint-no-root)#show context
meshpoint no-root
 meshid test
 beacon-format mesh-point
 control-vlan 1
 security-mode eap

```



```
root
nx9500-6C8809(config-device-B4-C7-99-71-17-28-meshpoint-no-root)#
```

## Related Commands

|                                                 |                                                                        |
|-------------------------------------------------|------------------------------------------------------------------------|
| <code>no (meshpoint-config)</code> on page 1780 | Removes the configuration of this meshpoint device as a root meshpoint |
|-------------------------------------------------|------------------------------------------------------------------------|

### *security-mode (meshpoint-config)*

Configures the security mode for this meshpoint

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
security-mode [eap|none|psk]
```

#### Parameters

```
security-mode [eap|none|psk]
```

|                            |                                                                                                                                                                                                                        |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>security-mode</code> | Configures the security mode for this meshpoint                                                                                                                                                                        |
| <code>eap</code>           | Uses 802.1X/EAP as the security mode. When using this option, use the <code>wpa2</code> command to specify the EAP authentication type and related parameters.                                                         |
| <code>none</code>          | No security is configured for this meshpoint                                                                                                                                                                           |
| <code>psk</code>           | Uses PSK (Pre Shared Key) as the security mode. When using this option, use the <code>wpa2</code> command to enter a 64 character HEX or an 8-63 ASCII character passphrase used for authentication on the mesh point. |

#### Examples

The following example shows root meshpoint configuration with PSK authentication enabled:

```
nx9500-6C8809(config-meshpoint-test)#security-mode psk
nx9500-6C8809(config-meshpoint-test)#show context
meshpoint test
description "This is an example of a meshpoint description"
meshid TestingMeshPoint
beacon-format mesh-point
control-vlan 1
allowed-vlans 1,10-16,18-23
neighbor inactivity-timeout 300
data-rates 2.4GHz bgn
data-rates 5GHz an
security-mode psk
root
nx9500-6C8809(config-meshpoint-test)#
```

The following example shows root meshpoint configuration with EAP authentication enabled:

```
nx9500-6C8809(config-meshpoint-root)#show context
meshpoint root
meshid test
```

```

beacon-format mesh-point
control-vlan 101
allowed-vlans 101,103
use aaa-policy test
security-mode eap
root
nx9500-6C8809(config-meshpoint-test)#

```

### Related Commands

|                                                 |                                                                                                                                   |
|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <code>no (meshpoint-config)</code> on page 1780 | Resets the security configuration for this meshpoint to “none”. This indicates that no security is configured for this meshpoint. |
|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|

### *service (meshpoint-config)*

Use this command to allow only those neighbors who are capable of 802.11n data rates to associate with this meshpoint.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
service [allow-ht-only|show cli]
```

#### Parameters

```
service [allow-ht-only|show cli]
```

|                                    |                                                                                                                                |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <code>service allow-ht-only</code> | Allows only those neighbors who are capable of high throughput data rates (802.11n data rates) to associate with the meshpoint |
| <code>service show cli</code>      | Displays running system configuration                                                                                          |

#### Examples

```

nx9500-6C8809(config-meshpoint-test)#service allow-ht-only
nx9500-6C8809(config-meshpoint-test)#show context
meshpoint test
description "This is an example of a meshpoint description"
meshid TestingMeshPoint
shutdown
beacon-format mesh-point
control-vlan 1
allowed-vlans 1,10-16,18-23
neighbor inactivity-timeout 300
data-rates 2.4GHz bgn
data-rates 5GHz an
security-mode psk
wpa2 psk 0 Test Company
wpa2 key-rotation unicast 1200
wpa2 key-rotation broadcast 600
root
service allow-ht-only
nx9500-6C8809(config-meshpoint-test)#

```

## Related Commands

|                                                    |                                                                                                      |
|----------------------------------------------------|------------------------------------------------------------------------------------------------------|
| <code>no (meshpoint-config)</code> on page 1780    | Removes the restriction that only 802.11n capable neighbor devices can associate with this meshpoint |
| <code>service</code> on page 647 (common commands) | Invokes service commands to troubleshoot or debug                                                    |

### *shutdown (meshpoint-config)*

Shuts down this meshpoint. Use this command to prevent an AP from participating in a mesh network.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
shutdown
```

#### Parameters

None

#### Examples

```
nx9500-6C8809(config-meshpoint-test)#shutdown
```

## Related Commands

|                                                 |                              |
|-------------------------------------------------|------------------------------|
| <code>no (meshpoint-config)</code> on page 1780 | Enables an AP as a meshpoint |
|-------------------------------------------------|------------------------------|

### *use (meshpoint-config)*

Uses a QoS (Quality of Service) policy defined specifically for meshpoints. To use this QoS policy, it must be defined.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
use [aaa-policy <AAA-POLICY-NAME>|meshpoint-qos-policy <MESHPOINT-QOS-POLICY-NAME>]
```

#### Parameters

```
use [aaa-policy <AAA-POLICY-NAME>|meshpoint-qos-policy <MESHPOINT-QOS-POLICY-NAME>]
```

|                                                     |                                                                                                                                                                                                                                     |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| meshpoint-qos-policy<br><MESHPOINT-QOS-POLICY-NAME> | Configures this meshpoint to use a predefined meshpoint QoS policy <ul style="list-style-type: none"> <li>&lt;MESHPOINT-QOS-POLICY-NAME&gt; - Specify the meshpoint QoS policy name (should be existing and configured).</li> </ul> |
| aaa-policy <AAA-POLICY-NAME>                        | Configures this meshpoint to use a predefined aaa-policy <ul style="list-style-type: none"> <li>&lt;AAA-POLICY-NAME&gt; - Specify the aaa-policy name (should be existing and configured).</li> </ul>                               |

## Examples

```

nx9500-6C8809(config-meshpoint-test)#use meshpoint-qos-policy test
nx9500-6C8809(config-meshpoint-test)#show context
meshpoint test
 description "This is an example of a meshpoint description"
 meshid TestingMeshPoint
 shutdown
 beacon-format mesh-point
 control-vlan 1
 allowed-vlans 1,10-16,18-23
 neighbor inactivity-timeout 300
 data-rates 2.4GHz bgn
 data-rates 5GHz an
 security-mode psk
 root
 use meshpoint-qos-policy test
nx9500-6C8809(config-meshpoint-test)#

```

## Related Commands

|                                                                   |                                                                 |
|-------------------------------------------------------------------|-----------------------------------------------------------------|
| <a href="#">no (meshpoint-config)</a> on page 1780                | Removes the meshpoint QoS policy associated with this meshpoint |
| <a href="#">meshpoint-qos-policy-config-instance</a> on page 1781 | Creates and configures a meshpoint QoS policy                   |
| <a href="#">AAA-POLICY</a> on page 1316                           | Creates and configures an AAA policy                            |

### *wpa2 (meshpoint-config)*

Use this command to configure the parameters of authentication mode specified using the 'security-mode' keyword. This command also allows you to set a unicast and broadcast key rotation interval.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```

wpa2 [eap|psk|key-rotation]
wpa2 key-rotation [broadcast|unicast] <30-86400>
wpa2 psk [0 <SECRET>|2 <SECRET>|<SECRET>]
wpa2 eap [auth-type|identity|peap-mschapv2|tls]
wpa2 eap [auth-type [peap-mschapv2|tls]|identity <WORD>]
wpa2 eap peap-mschapv2 user <USER-NAME> password [0 <WORD>|2 <WORD>|<WORD>]
{trustpoint <TRUSTPOINT-NAME>}
wpa2 eap tls trustpoint <TRUSTPOINT-NAME>

```

## Parameters

`wpa2 key-rotation [broadcast|unicast] <30-86400>`

|                                |                                                                                                                                                                                                                                                                                                                       |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>wpa2 key-rotation</code> | Enables periodic rotation of encryption keys used for broadcast and unicast traffic                                                                                                                                                                                                                                   |
| <code>broadcast</code>         | Configures key rotation interval for broadcast and multicast traffic. This option is disabled by default.<br>When enabled, the key indices used for encrypting/decrypting broadcast traffic is alternatively rotated based on the defined interval. Key rotation enhances the broadcast traffic security on the WLAN. |
| <code>unicast</code>           | Configures key rotation interval for unicast traffic. This option is disabled by default.                                                                                                                                                                                                                             |
| <code>&lt;30-86400&gt;</code>  | Configures key rotation interval from 30 - 86400 seconds for unicast or broadcast transmission                                                                                                                                                                                                                        |

`wpa2 psk [0 <SECRET>|2 <SECRET>|<SECRET>]`

|                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>wpa2 psk</code>                                                  | Configures the shared key for authentication mode PSK. If the security mode is set as 'psk' using the 'security-mode' keyword, use this command to configure the pre-shared key.                                                                                                                                                                                                                                                                 |
| <code>secret [0 &lt;SECRET&gt; 2 &lt;SECRET&gt; &lt;SECRET&gt;]</code> | Configures the PSK used to authenticate this meshpoint with other meshpoints in the network <ul style="list-style-type: none"><li>• 0 &lt;SECRET&gt; - Configures a clear text secret</li><li>• 2 &lt;SECRET&gt; - Configures an encrypted secret</li><li>• &lt;SECRET&gt; - Specify the secret key. The pre-shared key can be in ASCII (8 to 63 characters in length) or Hexadecimal (not exceeding 64 characters in length) formats.</li></ul> |

`wpa2 eap [auth-type [peap-mschapv2|tls]|identity <WORD>]`

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wpa2 eap                      | Configures the 802.1X/EAP based authentication type for this meshpoint. If the security mode is set as 'eap' using the 'security-mode' keyword, use this command to specify the EAP type. The options are: peap-mschapv2 and tls.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| auth-type [peap-mschapv2 tls] | <p>Specifies the EAP authentication type. The options are:</p> <ul style="list-style-type: none"> <li>peap-mschapv2 – Configures EAP authentication type as PEAP (Protected Extensible Authentication Protocol) with default auth type MSCHAPv2. This is the default setting.</li> </ul> <p>If using auth-type as 'peap-mschapv2', use the 'peap-mschapv2' keyword to configure user credentials and trustpoint details.</p> <ul style="list-style-type: none"> <li>tls – Configures EAP authentication type as TLS (Transport Layer Security)</li> </ul> <p>If using auth-type as 'tls', use the 'tls' keyword to configure trustpoint details.</p> <p><b>Note:</b> The certificate should be issued from an Enterprise or public certificate authority to allow 802.1X clients to validate the identity of the authentication server prior to forwarding credentials.</p> |
| identity <WORD>               | <p>Configures identity to be used during phase1 authentication</p> <ul style="list-style-type: none"> <li>&lt;WORD&gt; – Enter a string up to 256 characters in length (this should not be actual identity of user but some anonymous/bogus username).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

```
wpa2 eap peap-mschapv2 user <USER-NAME> password [0 <WORD>|2 <WORD>|<WORD>]
{trustpoint <TRUSTPOINT-NAME>}
```

|                                                      |                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wpa2 eap peap-mschapv2                               | Configures PEAP-related user credentials and trustpoint details                                                                                                                                                                                                                        |
| user <USER-NAME> password [0 <WORD> 2 <WORD> <WORD>] | <p>Specify the user credentials used for authentication</p> <ul style="list-style-type: none"> <li>user &lt;USER-NAME&gt; – Specify the user name</li> <li>password [0 &lt;WORD&gt; 2 &lt;WORD&gt; &lt;WORD&gt;] – Specify the password associated with the specified user.</li> </ul> |
| trustpoint <TRUSTPOINT-NAME>                         | <p>Optional. Associates a trustpoint used for installing CA certificate and verifying server certificate</p> <ul style="list-style-type: none"> <li>&lt;TRUSTPOINT-NAME&gt; – Specify the trustpoint name (should be existing and configured).</li> </ul>                              |

```
wpa2 eap tls trustpoint <TRUSTPOINT-NAME>
```

|                              |                                                                                                                                                                                                                                                                                                                                              |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wpa2 eap tls                 | Configures TLS client related parameters                                                                                                                                                                                                                                                                                                     |
| trustpoint <TRUSTPOINT-NAME> | <p>Configures trustpoint details trustpoint</p> <ul style="list-style-type: none"> <li>&lt;TRUSTPOINT-NAME&gt; – Assigns a trustpoint to be used for installing TLS client certificate, client private key, and CA certificate</li> <li>&lt;TRUSTPOINT-NAME&gt; – Specify the trustpoint name (should be existing and configured)</li> </ul> |

## Examples

```
nx9500-6C8809(config-meshpoint-test)#wpa2 key-rotation broadcast 600
nx9500-6C8809(config-meshpoint-test)#wpa2 key-rotation unicast 1200
nx9500-6C8809(config-meshpoint-test)#wpa2 psk Test Company
nx9500-6C8809(config-meshpoint-test)#show context
meshpoint test
description "This is an example of a meshpoint description"
```

```

meshid TestingMeshPoint
shutdown
beacon-format mesh-point
control-vlan 1
allowed-vlans 1,10-16,18-23
neighbor inactivity-timeout 300
data-rates 2.4GHz bgn
data-rates 5GHz an
security-mode psk
wpa2 psk 0 Test Company
wpa2 key-rotation unicast 1200
wpa2 key-rotation broadcast 600
root
nx9500-6C8809(config-meshpoint-test)#

```

The following example shows root meshpoint configuration with EAP authentication enabled:

```

nx9500-6C8809(config-meshpoint-root)#show context
meshpoint root
meshid test
beacon-format mesh-point
control-vlan 101
allowed-vlans 101,103
use aaa-policy test
security-mode eap
root
nx9500-6C8809(config-meshpoint-test)#

```

The following example shows non-root meshpoint configuration with EAP PEAP-MSCHAPv2 authentication:

```

nx9500-6C8809(config-meshpoint-testNoRoot)#show context
meshpoint testNoRoot
meshid test
beacon-format mesh-point
control-vlan 101
allowed-vlans 101,103
security-mode eap
wpa2 eap peap-mschapv2 user tester123 password 0 testing1234 trustpoint mesh1
wpa2 eap identity tester123
no root
nx9500-6C8809(config-meshpoint-testNoRoot)#

```

The following example shows non-root meshpoint configuration with EAP TLS authentication:

```

nx9500-6C8809(config-meshpoint-testNoRoot)#show context
meshpoint testNoRoot
meshid test
beacon-format mesh-point
control-vlan 101
allowed-vlans 101,103
security-mode eap
wpa2 eap peap-mschapv2 user tester123 password 0 testing1234 trustpoint mesh1
wpa2 eap tls trustpoint mesh1
wpa2 eap identity tester123
no root
nx9500-6C8809(config-meshpoint-testNoRoot)#

```

## Related Commands

|                                                                                                          |
|----------------------------------------------------------------------------------------------------------|
| <a href="#">no (meshpoint-config)</a> on page 1780    Resets PSK configuration and key rotation duration |
|----------------------------------------------------------------------------------------------------------|

*no (meshpoint-config)*

Negates meshpoint commands or resets their values to default

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
no [allowed-vlans|beacon-format|control-vlan|description|force|meshid|root|
security-mode|shutdown]
no data-rates [2.4GHz|5GHz]
no force peer-paths-through-root
no neighbor inactivity-timeout
no use [aaa-policy|meshpoint-qos-policy]
no wpa2 [eap|key-rotation|psk]
no wpa2 eap [auth-type|identity|peap-mschapv2|tls trustpoint]
no wpa2 key-rotation [broadcast|unicast]
no wpa2 psk
no service allow-ht-only
```

### Parameters

no <PARAMETERS>

|                 |                                                                                      |
|-----------------|--------------------------------------------------------------------------------------|
| no <PARAMETERS> | Removes or reverts this meshpoint settings to default based on the parameters passed |
|-----------------|--------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config-meshpoint-test)#show context
meshpoint test
 description "This is an example of a meshpoint description"
 meshid TestingMeshPoint
 shutdown
 beacon-format mesh-point
 control-vlan 1
 allowed-vlans 1,10-16,18-23
 neighbor inactivity-timeout 300
 data-rates 2.4GHz bgn
 data-rates 5GHz an
 security-mode psk
 wpa2 psk 0 Test Company
 wpa2 key-rotation unicast 1200
 wpa2 key-rotation broadcast 600
 root
nx9500-6C8809(config-meshpoint-test)#
nx9500-6C8809(config-meshpoint-test)#no allowed-vlans
nx9500-6C8809(config-meshpoint-test)#no beacon-format
nx9500-6C8809(config-meshpoint-test)#no control-vlan
nx9500-6C8809(config-meshpoint-test)#no description
nx9500-6C8809(config-meshpoint-test)#no meshid
nx9500-6C8809(config-meshpoint-test)#no root
nx9500-6C8809(config-meshpoint-test)#no security-mode
nx9500-6C8809(config-meshpoint-test)#show context
meshpoint test
 beacon-format mesh-point
 control-vlan 1
 neighbor inactivity-timeout 300
```



```

data-rates 2.4GHz bgn
data-rates 5GHz an
security-mode none
wpa2 psk 0 Test Company
wpa2 key-rotation unicast 1200
wpa2 key-rotation broadcast 600
no root
nx9500-6C8809(config-meshpoint-test)#no data-rates 2.4GHz
nx9500-6C8809(config-meshpoint-test)#no data-rates 5GHz
nx9500-6C8809(config-meshpoint-test)#show context
meshpoint test
 beacon-format mesh-point
 control-vlan 1
 neighbor inactivity-timeout 300
 security-mode none
 wpa2 psk 0 Test Company
 wpa2 key-rotation unicast 1200
 wpa2 key-rotation broadcast 600
 no root
nx9500-6C8809(config-meshpoint-test)#
rfs4000-229D58(config-meshpoint-test)#show context
meshpoint test
 meshid test
 beacon-format mesh-point
 control-vlan 1
 security-mode none
 no root
force peer-paths-through-root
rfs4000-229D58(config-meshpoint-test)#
rfs4000-229D58(config-meshpoint-test)#no force peer-paths-through-root
rfs4000-229D58(config-meshpoint-test)#show context
meshpoint test
 meshid test
 beacon-format mesh-point
 control-vlan 1
 security-mode none
 no root
rfs4000-229D58(config-meshpoint-test)#

```

## meshpoint-qos-policy-config-instance

Mesh QoS (Quality of Service) provides a data traffic prioritization scheme. QoS reduces congestion from excessive traffic. If there is enough bandwidth for all users and applications (unlikely because excessive bandwidth comes at a very high cost), then applying QoS has very little value. QoS provides policy enforcement for mission-critical applications and/or users that have critical bandwidth requirements when bandwidth is shared by different users and applications.

Mesh QoS helps ensure each mesh point on the mesh network receives a fair share of the overall bandwidth, either equally or as per the proportion configured. Packets directed towards clients are classified into categories such as video, voice and data packets within each category are processed based on the weights defined for each mesh point.

To create a meshpoint, see [meshpoint-config-instance](#) on page 1760.

A meshpoint QoS policy is created from the (config) instance. To create a meshpoint QoS policy use the following command:

```

<DEVICE>(config)#meshpoint-qos-policy <POLICY-NAME>
nx9500-6C8809(config)#meshpoint-qos-policy test
nx9500-6C8809(config-meshpoint-qos-test)#>

```

Mesh Point QoS Mode commands:

```
accelerated-multicast Configure accelerated multicast streams address and
 forwarding QoS classification
no Negate a command or set its defaults
rate-limit Configure traffic rate-limiting parameters on a
 per-meshpoint/per-neighbor basis

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal
```

```
nx9500-6C8809(config-meshpoint-qos-test)#
```

The following table summarizes the mespoint-qos-policy configuration commands.

**Table 62: Meshpoint-QoS-Policy Config Mode Commands**

| Command                                                                   | Description                                            |
|---------------------------------------------------------------------------|--------------------------------------------------------|
| <a href="#">accelerated-multicast (meshpoint-qos-policy)</a> on page 1782 | Configures accelerated multicast parameters            |
| <a href="#">rate-limit (meshpoint-qos-policy)</a> on page 1783            | Configures the rate limits for this QoS policy         |
| <a href="#">no (meshpoint-qos-policy)</a> on page 1786                    | Negates a command or reverts settings to their default |

### *accelerated-multicast (meshpoint-qos-policy)*

Configures the accelerated multicast stream's address and forwarding QoS classification

#### Note



For accelerated multicast feature to work, IGMP querier must be enabled. When a user joins a multicast stream, an entry is created in the device's (AP or wireless controller) snoop table and the entry is set to expire after a set time period. Multicast packets are forwarded to the appropriate wireless LAN or mesh until this entry is available in the snoop table. Snoop querier keeps the snoop table current by updating entries that are set to expire. It also keeps an entry for each multicast stream till there are users registered for the stream.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
accelerated-multicast [<MULTICAST-IP>|autodetect] {classification [background/best-effort|trust|video/voice]}
```

## Parameters

`accelerated-multicast [<MULTICAST-IP>|autodetect] {classification [background|best-effort|trust|video|voice]}`

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| accelerated-multicast | Configures the accelerated multicast stream address and forwarding QoS classification                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <MULTICAST-IP>        | Specify a list of multicast addresses and classifications. Packets are accelerated when the destination address matches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| autodetect            | Lets the system to automatically detect multicast streams to be accelerated<br>This option allows the administrator to convert multicast packets to unicast in order to provide better overall airtime utilization and performance. The system can be configured to automatically detect multicast streams and convert them to unicast, or specify which multicast streams are to be converted to unicast. When the stream is converted and being queued up for transmission, there are a number of classification mechanisms applied to the stream and the administrator can select what type of classification they would want. Classification types are trust, voice, video, best effort, and background. |
| classification        | Optional. Defines the QoS classification to apply to a multicast stream. The following options are available: <ul style="list-style-type: none"><li>• background</li><li>• best effort</li><li>• trust</li><li>• video</li><li>• voice</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## Examples

```
nx9500-6C8809(config-meshpoint-qos-test)#accelerated-multicast 224.0.0.1 classification video
nx9500-6C8809(config-meshpoint-qos-test)#show context
meshpoint-qos-policy test
 accelerated-multicast 224.0.0.1 classification video
nx9500-6C8809(config-meshpoint-qos-test)#
```

## Related Commands

|                                           |                                                                                     |
|-------------------------------------------|-------------------------------------------------------------------------------------|
| <code>no (meshpoint-qos-policy) on</code> | Resets accelerated multicast configurations for this meshpoint QoS policy page 1786 |
|-------------------------------------------|-------------------------------------------------------------------------------------|

### *rate-limit (meshpoint-qos-policy)*

Configures the rate limiting of traffic on a per meshpoint or per neighbor basis

Excessive traffic can cause performance issues or bring down the network entirely. Excessive traffic, bombardments and interference are caused by numerous sources, such as network loops, faulty devices, or malicious software (such as a worm or virus) that has infected one or more branch-level devices. Rate limiting limits the maximum rate sent to or received from the wireless network (and meshpoint) per neighbor. It prevents any single user from overwhelming the wireless network. It also provides differential service for service providers. An administrator can set separate QoS rate limit configurations for data transmitted from the network and data transmitted from a mesh point's neighbor.

Before defining rate limit thresholds for meshpoint transmit and receive traffic, it is recommended that you define the normal number of ARP, broadcast, multicast, and unknown unicast packets that typically

transmit and receive from each supported WMM access category. If thresholds are defined too low, normal network traffic (required by end-user devices) is dropped, resulting in intermittent outages and performance problems.

A connected neighbor can also have QoS rate limit settings defined in both the transmit and receive direction.

**Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

**Syntax**

```
rate-limit [meshpoint|neighbor]
rate-limit [meshpoint|neighbor] [from-air|to-air] {max-burst-size <2-1024>/rate
<50-1000000>}
rate-limit [meshpoint|neighbor] [from-air|to-air]
{red-threshold [background <0-100>/best-effort <0-100>/video <0-100>/voice <0-100>]}
```

**Parameters**

```
rate-limit [meshpoint|neighbor] [from-air|to-air] {max-burst-size <2-1024>/rate
<50-1000000>}
```

|           |                                                                                                                                                                                                                                   |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| meshpoint | Configures rate limit parameters for all data received from any meshpoint in the mesh network. This option is disabled by default.                                                                                                |
| neighbor  | Configures rate limit parameters for neighboring meshpoint devices. Enables rate limiting for data transmitted from the client to its associated access point radio and connected controller. This option is disabled by default. |
| from-air  | Configures rate limits for traffic from the wireless neighbor to the network.                                                                                                                                                     |
| to-air    | Configures rate limits for traffic from the network to the wireless neighbor.                                                                                                                                                     |

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| max-burst-size<br><2-1024> | <p>Optional. Configures the maximum burst size in kilobytes.</p> <ul style="list-style-type: none"> <li>• &lt;2-1024&gt; – Set a value from 2 - 1024 kbytes.</li> </ul> <p>For a meshpoint: The smaller the burst, the less likely that the transmit packet transmission results in congestion for the meshpoint's client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should then add a 10% margin (minimally) to allow for traffic bursts at the site. The default burst size is 320 kbytes.</p> <p>For a neighbor: The smaller the burst, the less likely the transmit packet transmission will result in congestion for the wireless client. The default burst size is 64 kbytes.</p> |
| rate<br><50-1000000>       | <p>Optional. Defines a receive or transmit rate limit in kilobytes per second</p> <ul style="list-style-type: none"> <li>• &lt;50-1000000&gt; – Set a value from 50 - 1000000 kbps.</li> </ul> <p>For a meshpoint: This limit constitutes a threshold for the maximum the number of packets transmitted or received over the meshpoint (from all access categories). Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 5000 kbps.</p> <p>For a neighbor: This limit constitutes a threshold for the maximum the number of packets transmitted or received (from all access categories). Traffic that exceeds the defined rate is dropped by the client and a log message is generated. The default rate is 1,000 kbps.</p>                                                                                                 |

```
rate-limit [meshpoint|neighbor] [from-air|to-air]
{red-threshold [background <0-100>|best-effort <0-100>|video <0-100>|voice <0-100>]}
```

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| meshpoint              | Configures rate limit parameters for a meshpoint                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| neighbor               | Configures rate limit parameters for neighboring meshpoint devices                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| from-air               | Configures rate limits for traffic from the wireless neighbor to the network                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| to-air                 | Configures rate limits for traffic from the network to the wireless neighbor                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| red-threshold          | Optional. Configures RED (random early detection) threshold for traffic class                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| background<br><0-100>  | <p>The following keyword is applicable to the 'from-air' and 'to-air' traffics.</p> <ul style="list-style-type: none"> <li>• background &lt;0-100&gt; – Configures the threshold for low priority (background) traffic</li> <li>• &lt;0-100&gt; – Specify a value from 0 - 100.</li> </ul> <p>For a meshpoint: This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped and a log message is generated. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general transmit rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.</p> <p>For a neighbor: This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 50%.</p> |
| best-effort<br><0-100> | <p>The following keyword is applicable to the 'from-air' and 'to-air' traffics.</p> <ul style="list-style-type: none"> <li>• best-effort &lt;0-100&gt; – Configures the threshold for best-effort traffic</li> <li>• &lt;0-100&gt; – Specify a value from 0 - 100.</li> </ul> <p>For a meshpoint: This is a percentage of the maximum burst size for normal priority traffic. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general transmit rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.</p> <p>For a neighbor: This is a percentage of the maximum burst size for normal traffic. Best effort traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 50%.</p>                                        |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>video &lt;0-100&gt; The following keyword is applicable to the 'from-air' and 'to-air' traffics.</p> <ul style="list-style-type: none"> <li>best-effort &lt;0-100&gt; – Configures the threshold for video traffic <ul style="list-style-type: none"> <li>&lt;0-100&gt; – Specify a value from 0 - 100.</li> </ul> </li> </ul> <p>For a meshpoint: This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped and a log message is generated. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general transmit rate is known by the network administrator (using a time trend analysis). The default threshold is 25%.</p> <p>For a neighbor: This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 25%.</p>                                          |
| <p>voice &lt;0-100&gt; The following keyword is applicable to the 'from-air' and 'to-air' traffics.</p> <ul style="list-style-type: none"> <li>voice &lt;0-100&gt; – Configures the threshold for voice traffic <ul style="list-style-type: none"> <li>&lt;0-100&gt; – Specify a value from 0 - 100.</li> </ul> </li> </ul> <p>For a meshpoint: This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped and a log message is generated. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 0%.</p> <p>For a neighbor: This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 0% and implies no early random drops will occur.</p> |

### Examples

```

nx9500-6C8809(config-meshpoint-qos-test)#rate-limit meshpoint from-air max-burst-size 800
nx9500-6C8809(config-meshpoint-qos-test)#show context
meshpoint-qos-policy test
 rate-limit meshpoint from-air max-burst-size 800
 accelerated-multicast 224.0.0.1 classification video
nx9500-6C8809(config-meshpoint-qos-test)#
nx9500-6C8809(config-meshpoint-qos-test)#rate-limit meshpoint from-air rate 80000
nx9500-6C8809(config-meshpoint-qos-test)#rate-limit meshpoint from-air red-threshold video
80
nx9500-6C8809(config-meshpoint-qos-test)#rate-limit meshpoint from-air red-threshold voice
70
nx9500-6C8809(config-meshpoint-qos-test)#show context
meshpoint-qos-policy test
 rate-limit meshpoint from-air rate 80000
 rate-limit meshpoint from-air max-burst-size 800
 rate-limit meshpoint from-air red-threshold video 80
 rate-limit meshpoint from-air red-threshold voice 70
 accelerated-multicast 224.0.0.1 classification video
nx9500-6C8809(config-meshpoint-qos-test)#

```

### Related Commands

|                                                        |                                                          |
|--------------------------------------------------------|----------------------------------------------------------|
| <a href="#">no (meshpoint-qos-policy)</a> on page 1786 | Resets traffic rate limits for this meshpoint QoS policy |
|--------------------------------------------------------|----------------------------------------------------------|

*no (meshpoint-qos-policy)*

Negates the commands for meshpoint QoS policy or resets their values to their default

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
no [accelerated-multicast|rate-limit]
no accelerated-multicast [<MULTICAST-IP>|autodetect]
no rate-limit [meshpoint|neighbor] [from-air|to-air] {max-burst-size|rate}
no rate-limit [meshpoint|neighbor] [from-air|to-air] {red-threshold [background|
best-effort|video|voice]}
```

### Parameters

```
no <PARAMETERS>
```

```
no <PARAMETERS> Removes or reverts this meshpoint QoS policy settings to default based on the parameters
passed
```

### Examples

```
nx9500-6C8809(config-meshpoint-qos-test)#show context
meshpoint-qos-policy test
 rate-limit meshpoint from-air rate 80000
 rate-limit meshpoint from-air red-threshold video 80
 rate-limit meshpoint from-air red-threshold voice 70
 accelerated-multicast 224.0.0.1 classification video
nx9500-6C8809(config-meshpoint-qos-test)#
nx9500-6C8809(config-meshpoint-qos-test)#no rate-limit meshpoint from-air rate
nx9500-6C8809(config-meshpoint-qos-test)#no rate-limit meshpoint from-air red-threshold
video 80
nx9500-6C8809(config-meshpoint-qos-test)#no rate-limit meshpoint from-air red-threshold
voice 70
nx9500-6C8809(config-meshpoint-qos-test)#show context
meshpoint-qos-policy test
 accelerated-multicast 224.0.0.1 classification video
nx9500-6C8809(config-meshpoint-qos-test)#
```

## meshpoint-device-config-instance

This `meshpoint-device` command configures an access point to use a defined meshpoint. To configure this feature use one of the following options:

- navigate to the device profile config context (used when configuring access point profile on a controller)
- navigate to the device's config context using the self command (used when configuring a logged on access point)

*Supported in the following platforms:*

- Access Points — AP 6522, AP 6532, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 81XX

### Syntax

```
meshpoint-device <MESHPOINT-NAME>
```

## Parameters

meshpoint-device <MESHPOINT-NAME>

|                  |                                                                                                 |
|------------------|-------------------------------------------------------------------------------------------------|
| meshpoint-device | Configures the AP as a meshpoint device and sets its parameters                                 |
| <MESHPOINT-NAME> | Specify the name of the meshpoint to configure the AP with (should be existing and configured). |

## Example

In the following examples, the meshpoint is applied to an access point profile.

```
nx9500-6C8809(config)#profile ap8432 testAP8432
nx9500-6C8809(config-profile-testAP8432)#meshpoint-device TestMeshpoint
nx9500-6C8809(config-profile-testAP8432-meshpoint-TestMeshpoint)#?
```

Mesh Point Device Mode commands:

```
acs Configure auto channel selection parameters
exclude Exclude neighboring Mesh Devices
hysteresis Configure path selection SNR hysteresis values
monitor Event Monitoring
no Negate a command or set its defaults
path-method Path selection method used to find a root node
preferred Configure preferred path parameters
root Set this meshpoint as root
root-select Root selection method parameters

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal
```

```
nx9500-6C8809(config-profile-testAP8432-meshpoint-TestMeshpoint)#
ap8432-070235(config-device-74-67-F7-07-02-35)#meshpoint-device test
ap8432-070235(config-device-74-67-F7-07-02-35-meshpoint-test)#?
```

Mesh Point Device Mode commands:

```
acs Configure auto channel selection parameters
exclude Exclude neighboring Mesh Devices
hysteresis Configure path selection SNR hysteresis values
monitor Event Monitoring
no Negate a command or set its defaults
path-method Path selection method used to find a root node
preferred Configure preferred path parameters
root Set this meshpoint as root
root-select Root selection method parameters

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal
```

```
ap8432-070235(config-device-74-67-F7-07-02-35-meshpoint-test)#
```



The following table summarizes the meshpoint-device configuration mode commands.

**Table 63: Meshpoint-Device Config Commands**

| Command                                                            | Description                                                                             |
|--------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| <a href="#">acs (meshpoint-device-config)</a> on page 1789         | Enables ACS (Automatic Channel Selection) on this meshpoint device (access point)       |
| <a href="#">exclude (meshpoint-device-config)</a> on page 1794     | Excludes neighboring mesh devices                                                       |
| <a href="#">hysteresis (meshpoint-device-config)</a> on page 1795  | Configures path selection SNR hysteresis values on this meshpoint-device (Access Point) |
| <a href="#">monitor (meshpoint-device-config)</a> on page 1796     | Enables monitoring of critical resource and primary port links on a meshpoint device    |
| <a href="#">path-method (meshpoint-device-config)</a> on page 1796 | Configures the method used to select the path to the root node in a mesh network        |
| <a href="#">preferred (meshpoint-device-config)</a> on page 1797   | Configures the preferred path parameters for a meshpoint device                         |
| <a href="#">root (meshpoint-device-config)</a> on page 1799        | Configures a meshpoint device as the root meshpoint                                     |
| <a href="#">root-select (meshpoint-device-config)</a> on page 1798 | Configures this meshpoint device as the cost root                                       |
| <a href="#">no (meshpoint-device-config)</a> on page 1800          | Negates the commands for a meshpoint device or resets values to default                 |

#### *acs (meshpoint-device-config)*

Enables ACS (Automatic Channel Selection) on this meshpoint device (access point). When enabled, this feature automatically selects the best channel for a meshpoint-device radio based on the device configuration, channel conditions, and network layout.

In a wireless network deployment, it is advantageous for network devices to have the ability to operate in multiple channels and not be limited to only a single channel. Multiple channels increase the bandwidth and throughput of the wireless network. In such a scenario, each network device must have a mechanism to dynamically select a suitable channel of operation. ACS provides the required mechanism for a MCX enabled device.

Use this command to configure the ACS settings and override the default meshpoint configurations.

#### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6532, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7632, AP 7662, AP 8432, AP 8533

## Syntax

```
acs [channel-hold-time|channel-switch-delta|channel-width|ocs-duration|ocs-frequency|
path-min|path-threshold|preferred-interface-tolerance-period|preferred-radio-interface|
priority-meshpoint|sample-count|snr-delta|signal-threshold|tolerance-period]
acs channel-hold-time [2.4GHz|5GHz] <0-86400>
acs channel-switch-delta [2.4GHz|5GHz] <5-35>
acs channel-width [2.4GHz|5GHz] [20MHz|40MHz|80MHz|auto]
acs ocs-duration [2.4GHz|5GHz] <20-250>
acs ocs-frequency [2.4GHz|5GHz] <1-60>
acs path-min [2.4GHz|5GHz] <100-20000>
acs path-threshold [2.4GHz|5GHz] <800-65535>
acs preferred-interface-tolerance-period [2.4GHz|5GHz] <10-600>
acs preferred-radio-interface [2.4GHz|5GHz] <0-2>
acs priority-meshpoint [2.4GHz|5GHz] <MESHPOINT-NAME>
acs priority-meshpoint [2.4GHz|5GHz] <MESHPOINT-NAME>
acs sample-count [2.4GHz|5GHz] <1-10>
acs snr-delta [2.4GHz|5GHz] <1-100>
acs signal-threshold [2.4GHz|5GHz] <-100-0>
acs tolerance-period [2.4GHz|5GHz] <10-600>
```

## Parameters

```
acs channel-hold-time [2.4GHz|5GHz] <0-86400>
```

|                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| acs                                       | Configures ACS settings and overrides on the selected meshpoint-device                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| channel-hold-time [2.4GHz 5GHz] <0-86400> | <p>Configures the minimum time, in seconds, before a periodic scan, to assess channel conditions for a meshpoint root, is triggered.</p> <ul style="list-style-type: none"><li>2.4 GHz – Configures the channel hold interval for the 2.4 GHz radio band</li><li>5.0GHz – Configures the channel hold interval for the 5.0 GHz radio band</li></ul> <p>The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands:</p> <ul style="list-style-type: none"><li>&lt;0-86400&gt; – Specify a value from 0 - 86400 seconds. The default is 1800 seconds.</li></ul> <p><b>Note:</b> A value of '0' disables periodic channel assessment.</p> |

```
acs channel-switch-delta [2.4GHz|5GHz] <5-35>
```

|                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| acs                                       | Configures ACS settings and overrides on the selected meshpoint-device                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| channel-switch-delta [2.4GHz 5GHz] <5-35> | <p>Configures the difference in interference between the current and best channel needed to trigger a channel change. Once the difference in the current channel and the best channel interference equals the configured value, a channel change is triggered.</p> <ul style="list-style-type: none"><li>2.4 GHz – Configures the channel switch delta for the 2.4GHz radio band</li><li>5.0GHz – Configures the channel switch delta for the 5.0 GHz radio band</li></ul> <p>The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands:</p> <ul style="list-style-type: none"><li>&lt;5-35&gt; – Specify a value from 5 - 35 dBm. The default is 10 dBm.</li></ul> |

```
acs channel-width [2.4GHz|5GHz] [20MHz|40MHz|80MHz|auto]
```

|                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| acs                                                    | Configures ACS settings and overrides on the selected meshpoint-device                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| channel-width [2.4GHz 5GHz] [20MHz] 40MHz 80MHz  auto] | <p>Configures the channel width that meshpoint auto channel selection assigns to the radio</p> <ul style="list-style-type: none"> <li>• 2.4 GHz – Configures the operating channel width for the 2.4 GHz radio band</li> <li>• 5.0 GHz – Configures the operating channel width for the 5.0 GHz radio band</li> </ul> <p>The following keywords are common to the '2.4 GHz' and '5.0 GHz' bands:</p> <ul style="list-style-type: none"> <li>• 20 MHz – Assigns the 20 MHz channel width to the radio</li> <li>• 40 MHz – Assigns the 40 MHz channel width to the radio</li> <li>• auto – Selects and assigns the best possible channel from the 20/40 MHz width. This is the default setting.</li> </ul> |

acs ocs-duration [2.4GHz|5GHz] <20-250>

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| acs                                 | Configures ACS settings and overrides on the selected meshpoint-device                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| ocs-duration [2.4GHz 5GHz] <20-250> | <p>Configures the duration, in milliseconds, of OCSs (off -channel scans)</p> <ul style="list-style-type: none"> <li>• 2.4 GHz – Configures the ocs-duration for the 2.4 GHz radio band</li> <li>• 5.0 GHz – Configures the ocs-duration for the 5.0 GHz radio band</li> </ul> <p>The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands:</p> <ul style="list-style-type: none"> <li>• &lt;20-250&gt; – Specify a value from 20 - 250 milliseconds. The default value is 50 milliseconds.</li> </ul> |

acs ocs-frequency [2.4GHz|5GHz] <1-60>

|                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| acs                                | Configures ACS settings and overrides on the selected meshpoint-device                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| ocs-frequency [2.4GHz 5GHz] <1-60> | <p>Configures the interval, in seconds, at which off-channel scan is performed. An ocs-frequency of 10 seconds means that an off-channel scan will be performed once every 10 seconds.</p> <ul style="list-style-type: none"> <li>• 2.4 GHz – Configures the ocs-frequency for the 2.4 GHz radio band</li> <li>• 5.0 GHz – Configures the ocs-frequency for the 5.0 GHz radio band</li> </ul> <p>The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands:</p> <ul style="list-style-type: none"> <li>• &lt;1-60&gt; – Specify a value form 1 - 60 seconds. The default is 6 seconds.</li> </ul> |

acs path-min [2.4GHz|5GHz] <100-20000>

|                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| acs                                | Configures ACS settings and overrides on the selected meshpoint-device                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| path-min [2.4GHz 5GHz] <100-20000> | <p>Configures the minimum root path metric needed for auto channel selection. This is the acceptance root path metric value to consider a root as a possible candidate mesh node.</p> <ul style="list-style-type: none"> <li>• 2.4 GHz – Configures the minimum root path metric for the 2.4 GHz radio band</li> <li>• 5.0 GHz – Configures the minimum root path metric for the 5.0 GHz radio band</li> </ul> <p>The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands:</p> <ul style="list-style-type: none"> <li>• &lt;100-20000&gt; – Specify a value from 100 - 20000. The default is 1000.</li> </ul> |

acs path-threshold [2.4GHz|5GHz] <800-65535>

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| acs                                      | Configures ACS settings and overrides on the selected meshpoint-device                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| path-threshold [2.4GHz 5GHz] <800-65535> | <p>Configures the root path metric threshold for auto channel selection. This is the acceptance root path metric threshold beyond which the root bound to is considered as bad.</p> <ul style="list-style-type: none"> <li>• 2.4 GHz – Configures the root path metric threshold for the 2.4 GHz radio band</li> <li>• 5.0 GHz – Configures the root path metric threshold for the 5.0 GHz radio band</li> </ul> <p>The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands:</p> <ul style="list-style-type: none"> <li>• &lt;800-65535&gt; – Specify a value from 800 -65535. The default is 1500.</li> </ul> |

acs preferred-interface-tolerance-period [2.4GHz|5GHz] <10-600>

|                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| acs                                                         | Configures ACS settings and overrides on the selected meshpoint-device                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| preferred-interface-tolerance-period [2.4GHz 5GHz] <10-600> | <p>Configures the maximum tolerance period, in seconds, for low root metrics on the preferred interface. This is the duration to wait before triggering an automatic channel selection for the next mesh-hop on the preferred interface.</p> <ul style="list-style-type: none"> <li>• 2.4 GHz – Configures the maximum tolerance period for the 2.4 GHz radio band</li> <li>• 5.0 GHz – Configures the maximum tolerance period for the 5.0 GHz radio band</li> </ul> <p>The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands:</p> <ul style="list-style-type: none"> <li>• &lt;800-65535&gt; – Specify a value from 10 - 600 seconds.</li> </ul> |

acs preferred-radio-interface [2.4GHz|5GHz] <0-2>

|                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| acs                                           | Configures ACS settings and overrides on the selected meshpoint-device                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| preferred-radio-interface [2.4GHz 5GHz] <0-2> | <p>Configures the preferred radio interface on dual band APs</p> <ul style="list-style-type: none"> <li>• 2.4 GHz – Configures the preferred radio interface for the 2.4 GHz radio band</li> <li>• 5.0 GHz – Configures the preferred radio interface for the 5.0 GHz radio band</li> </ul> <p>The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands:</p> <ul style="list-style-type: none"> <li>• &lt;0-2&gt; – Specify a value form 0 - 2. A value of 0 (zero) indicates no preferred radio.</li> </ul> |

acs priority-meshpoint [2.4GHz|5GHz] <MESHPOINT-NAME>

|                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| acs                                                         | Configures ACS settings and overrides on the selected meshpoint-device                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| priority-meshpoint<br>[2.4GHz 5GHz]<br><MESHPOINT-<br>NAME> | <p>Configures the priority meshpoint. Configuring a priority meshpoint overrides automatic meshpoint configuration.</p> <ul style="list-style-type: none"> <li>• 2.4 GHz – Configures the priority meshpoint for the 2.4 GHz radio band</li> <li>• 5.0 GHz – Configures the priority meshpoint for the 5.0 GHz radio band</li> </ul> <p>The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands:</p> <ul style="list-style-type: none"> <li>• &lt;MESHPOINT-NAME&gt; – Specify the meshpoint name for the selected radio band.</li> </ul> |

acs sample-count [2.4GHz|5GHz] <1-10>

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| acs                                     | Configures ACS settings and overrides on the selected meshpoint-device                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| sample-count<br>[2.4GHz 5GHz]<br><1-10> | <p>Configures the minimum number of scan cycle samples to consider for auto channel selection</p> <ul style="list-style-type: none"> <li>• 2.4 GHz – Configures the sample count for the 2.4 GHz radio band</li> <li>• 5.0 GHz – Configures the sample count for the 5.0 GHz radio band</li> </ul> <p>The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands:</p> <ul style="list-style-type: none"> <li>• &lt;1-10&gt; – Specify a value from 1 -10. The default is 5 samples.</li> </ul> |

acs snr-delta [2.4GHz|5GHz] <1-100>

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| acs                                    | Configures ACS settings and overrides on the selected meshpoint-device                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| snr-delta<br>[2.4GHz <br>5GHz] <1-100> | <p>Configures the channel SNR delta. A meshpoint on a candidate channel must have a SNR of a greater delta than the next hop on the current channel.</p> <ul style="list-style-type: none"> <li>• 2.4 GHz – Configures the snr-delta for the 2.4 GHz radio band</li> <li>• 5.0 GHz – Configures the snr-delta for the 5.0 GHz radio band</li> </ul> <p>The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands:</p> <ul style="list-style-type: none"> <li>• &lt;1-100&gt; – Specify a value from 1 - 100 dB. The default is 5 dB.</li> </ul> |

acs snr-threshold [2.4GHz|5GHz] <-100-0>

|                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| acs                                        | Configures ACS settings and overrides on the selected meshpoint-device                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| snr-threshold<br>[2.4GHz 5GHz]<br><-100-0> | <p>Configures the signal strength threshold. If the signal strength of the next hop drops below the configured snr-threshold, a scan is triggered.</p> <ul style="list-style-type: none"> <li>• 2.4 GHz – Configures the snr-threshold for the 2.4 GHz radio band</li> <li>• 5.0 GHz – Configures the snr-threshold for the 5.0 GHz radio band</li> </ul> <p>The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands:</p> <ul style="list-style-type: none"> <li>• &lt;-100-0&gt; – Specify a value from -100 - 0 dB. The default is -65 dB.</li> </ul> |

acs tolerance-period [2.4GHz|5GHz] <10-600>

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| acs                                     | Configures ACS settings and overrides on the selected meshpoint-device                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| tolerance-period [2.4GHz 5GHz] <10-600> | <p>Configures the maximum tolerance period in seconds. This is the interval to wait for the root bound to recovery from a bad link.</p> <ul style="list-style-type: none"> <li>2.4 GHz - Configures the tolerance-period for the 2.4 GHz radio band</li> <li>5.0 GHz - Configures the tolerance-period for the 5.0 GHz radio band</li> </ul> <p>The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands:</p> <ul style="list-style-type: none"> <li>&lt;10-600&gt; - Specify a value from 10 - 600 seconds. the default is 60 seconds.</li> </ul> |

### Examples

```
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#acs channel-hold-time 2.4GHz 2500
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#acs ocs-duration 2.4GHz 30
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#acs ocs-frequency 2.4GHz 1
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#show context
meshpoint-device test
 acs ocs-frequency 2.4GHz 1
 acs ocs-duration 2.4GHz 30
 acs channel-hold-time 2.4GHz 2500
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#
```

### Related Commands

|                                                        |                                                |
|--------------------------------------------------------|------------------------------------------------|
| <code>no (meshpoint-device-config)</code> on page 1800 | Reverts the configured ACS settings to default |
|--------------------------------------------------------|------------------------------------------------|

*exclude (meshpoint-device-config)*

Enables wired-peer (that are wired MiNT level-1 neighbors) exclusion

### Supported in the following platforms:

- Access Points — AP 6522, AP 6532, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7632, AP 7662, AP 8432, AP 8533

### Syntax

```
exclude wired-peer mint-level-1
```

### Parameters

```
exclude wired-peer mint-level-1
```

|                         |                                                                                                                                                 |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| exclude wired-peer      | Excludes neighboring mesh devices                                                                                                               |
| wired-peer mint-level-1 | Excludes neighboring wired mesh devices with MiNTlevel-1 link<br>When enabled, all neighboring wired mesh devices are excluded from mesh links. |

### Examples

```
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#exclude wired-peer mint-level-1
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#show context
meshpoint-device test
 exclude wired-peer mint-level-1
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#
```

## Related Commands

`no (meshpoint-device-config)` on page 1800 Disables wired-peer exclusion on this meshpoint

### *hysteresis (meshpoint-device-config)*

Configures path selection SNR hysteresis values on this meshpoint-device (access point). These are settings that facilitate dynamic path selection. Configuring hysteresis prevents frequent re-ranking of the shortest path cost.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6532, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7632, AP 7662, AP 8432, AP 8533

#### Syntax

```
hysteresis [min-threshold|period|root-sel-snr-delta|snr-delta]
hysteresis [min-threshold <-100-0>|period <0-600>|root-sel-snr-delta <1-100>|
snr-delta <1-100>]
```

#### Parameters

```
hysteresis [min-threshold <-100-0>|period <0-600>|root-sel-snr-delta <1-100>|
snr-delta <1-100>]
```

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| min-threshold<br><-100-0>     | Configures the minimum signal strength that a device should have to be considered a likely candidate in the mesh route (to the mesh root node) selection process. <ul style="list-style-type: none"><li>• &lt;-100-0&gt; - Specify a value from -100 - 0 dB. The default is 0 dB.</li></ul>                                                                                                                                     |
| period<br><0-600>             | Configures the interval, in seconds, for which a likely candidate's path method hysteresis is sustained. In other words a device capable of sustaining the signal strength for the specified period of time is a likely candidate in the mesh route (to the mesh root node) selection process. <ul style="list-style-type: none"><li>• &lt;0-600&gt; - Specify a value from 0 - 600 seconds. The default is 1 second.</li></ul> |
| root-sel-snr-delta<br><1-100> | Configures the signal strength, in dB, that a device has to sustain, within the delta range, to be considered a likely candidate in the mesh route (to the mesh root node) selection process. <ul style="list-style-type: none"><li>• &lt;1-100&gt; - Specify a value from 1 - 100 dB.</li></ul>                                                                                                                                |
| snr-delta<br><1-100>          | Configures the SNR delta. The device with must have a SNR of a greater delta than its current neighbor to be considered a likely candidate in the mesh route (to the mesh root) selection process. <ul style="list-style-type: none"><li>• &lt;1-100&gt; - Specify a value from 1 - 100 dB. The default is 1 dB.</li></ul>                                                                                                      |

#### Examples

```
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#hysteresis period 15
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#hysteresis root-sel-snr-delta 12
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#hysteresis snr-delta 3
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#hysteresis min-threshold -65
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#show context
meshpoint-device test
 hysteresis period 15
 hysteresis snr-delta 3
 hysteresis min-threshold -65
 hysteresis root-sel-snr-delta 12
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#
```

## Related Commands

`no (meshpoint-device-config)` on page 1800 Removes the configured path selection SNR hysteresis values

### *monitor (meshpoint-device-config)*

Enables monitoring of critical resource and primary port links. It also configures the action taken in case a critical resource goes down or a primary port link is lost.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6532, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7632, AP 7662, AP 8432, AP 8533

#### Syntax

```
monitor [critical-resource|primary-port-link-loss] action no-root
```

#### Parameters

```
monitor [critical-resource|primary-port-link-loss] action no-root
```

|                        |                                                                                                                                                                                                                                                                                                                                           |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| critical-resource      | Enables critical resource down event monitoring                                                                                                                                                                                                                                                                                           |
| primary-port-link-loss | Enables primary port link loss event monitoring                                                                                                                                                                                                                                                                                           |
| action                 | The following are common to all of the above: <ul style="list-style-type: none"><li>• action - Sets the action taken if a critical resource goes down or if a primary port link is lost</li><li>• no-root - Changes the meshpoint to be non root (this is the action taken in case any of the above mentioned two events occur)</li></ul> |

#### Examples

```
nx9500-6C8809(config-profile-AP71XXTestProfile-meshpoint-test)#monitor critical-resource
action no-root
nx9500-6C8809(config-profile-AP71XXTestProfile-meshpoint-test)#show context
meshpoint-device test
name test
monitor critical-resource action no-root
nx9500-6C8809(config-profile-AP71XXTestProfile-meshpoint-test)#
```

## Related Commands

`no (meshpoint-device-config)` on page 1800 Disables monitoring of critical resource and primary port links.

### *path-method (meshpoint-device-config)*

Configures the path selection method used on a meshpoint device. This is the method used to select the route to the root node within a mesh network.



### Supported in the following platforms:

- Access Points — AP 6522, AP 6532, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7632, AP 7662, AP 8432, AP 8533

### Syntax

```
path-method [bound-pair|mobile-snr-leaf|snr-leaf|uniform]
```

### Parameters

```
path-method [bound-pair|mobile-snr-leaf|snr-leaf|uniform]
```

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| path-method     | Sets the method used to select the path to the root node in a mesh network                                                                                                                                                                                                                                                                                                                                                                                                              |
| bound-path      | Enables a meshpoint to form an exclusive path with only one other meshpoint. Select this option to bind one mesh point connection at a time. Once established, other mesh point connection requests are denied.                                                                                                                                                                                                                                                                         |
| mobile-snr-leaf | Configures the path selection method as mobile-snr-leaf. When selected, the path to the root node is selected based on the SNR (Signal-to-Noise Ratio) to a neighboring device. This option allows meshpoint devices to select a neighbor with the strongest SNR. Meshpoint devices using the mobile-snr-leaf method are non-forwarding nodes in the meshpoint traffic.<br><br><b>Note:</b> Select this option for VMM (Vehicular Mounted Modem) access points or other mobile devices. |
| snr-leaf        | This option allows meshpoints to select a neighbor with the strongest SNR. It is similar to the mobile-snr-leaf option, but is not applicable to mobile devices, such as VMMs.                                                                                                                                                                                                                                                                                                          |
| uniform         | Indicates the path selection method is uniform. When selected, two paths will be considered equivalent if the average goodput is the same for both paths. This is the default setting.<br><br><b>Note:</b> Select this option for infrastructure devices.                                                                                                                                                                                                                               |

### Examples

```
nx9500-6C8809(config-profile-AP71XXTestProfile-meshpoint-test)#path-method mobile-snr-leaf
nx9500-6C8809(config-profile-AP71XXTestProfile-meshpoint-test)#show context
meshpoint-device TEST
 name TEST
 path-method mobile-snr-leaf
nx9500-6C8809(config-profile-AP71XXTestProfile-meshpoint-test)#
```

*preferred (meshpoint-device-config)*

Configures the preferred path parameters for this meshpoint device

### Supported in the following platforms:

- Access Points — AP 6522, AP 6532, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7632, AP 7662, AP 8432, AP 8533

### Syntax

```
preferred [neighbor <MAC>|root <MAC>|interface [2.4GHz|4.9GHz|5GHz]]
```

### Parameters

```
preferred [neighbor <MAC>|root <MAC>|interface [2.4GHz|4.9GHz|5GHz]]
```

|                                |                                                                      |
|--------------------------------|----------------------------------------------------------------------|
| preferred                      | Configures the preferred path parameters                             |
| neighbor <MAC>                 | Adds the MAC address of a neighbor meshpoint as a preferred neighbor |
| root <MAC>                     | Adds the MAC address of a root meshpoint as a preferred root         |
| interface [2.4GHz 4.9GHz 5GHz] | Sets the preferred interface                                         |

### Examples

```

nx9500-6C8809(config-profile-AP71XXTestProfile-meshpoint-test)#preferred neighbor
11-22-33-44-55-66
nx9500-6C8809(config-profile-AP71XXTestProfile-meshpoint-test)#preferred root
22-33-44-55-66-77
nx9500-6C8809(config-profile-AP71XXTestProfile-meshpoint-test)#preferred interface 5GHz
nx9500-6C8809(config-profile-AP71XXTestProfile-meshpoint-test)#show context
meshpoint-device test
 name test
 preferred root 22-33-44-55-66-77
 preferred neighbor 11-22-33-44-55-66
 preferred interface 5GHz
 monitor critical-resource action no-root
nx9500-6C8809(config-profile-AP71XXTestProfile-meshpoint-test)#

```

### Related Commands

|                                              |                                                                        |
|----------------------------------------------|------------------------------------------------------------------------|
| <code>no (meshpoint-device-config) on</code> | Removes the configuration of preferred paths for this meshpoint device |
| page 1800                                    |                                                                        |

### *root-select (meshpoint-device-config)*

Configures this mesh-point device as the cost. root

### Supported in the following platforms:

- Access Points — AP 6522, AP 6532, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7632, AP 7662, AP 8432, AP 8533

### Syntax

```
root-select cost-root
```

### Parameters

```
root-select cost-root
```

|             |                                                                                                                                         |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| root-select | Configures this meshpoint device as the cost root. This is necessary for dynamic root selection                                         |
| cost-root   | process.<br>Select this option to set the meshpoint as the cost root for meshpoint root selection. This setting is disabled by default. |

### Examples

```

ap8432-070235(config-device-74-67-F7-07-02-35-meshpoint-test)#root-select cost-root
ap8432-070235(config-device-74-67-F7-07-02-35-meshpoint-test)#show context
meshpoint-device test
 root select-method auto-mint
 root-select cost-root
ap8432-070235(config-device-74-67-F7-07-02-35-meshpoint-test)#

```

## Related Commands

`no (meshpoint-device-config)` on page 1800 Removes this mesh-point device as the cost. root.

### *root (meshpoint-device-config)*

Configures this meshpoint device as the root meshpoint

You can optionally use the `select-method` option to enable dynamic mesh selection. When enabled, this option overrides `root` or `no-root` configuration and uses the selection method.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6532, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7632, AP 7662, AP 8432, AP 8533

### Syntax

```
root {select-method [auto-mint|auto-proximity]}
```

### Parameters

```
root {select-method [auto-mint|auto-proximity]}
```

|                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>root</code>                         | Configures this meshpoint device as the root meshpoint                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <code>select-method auto-mint]</code>     | <p>Optional. Enables dynamic mesh selection. When enabled, this option overrides <code>root</code> or <code>no-root</code> configuration and chooses the selection method.</p> <ul style="list-style-type: none"><li>• <code>auto-mint</code> - Enables dynamic root selection using Auto-MiNT (based on path cost)</li></ul> <p>The Auto-Mint or Cost Method dynamically determines the root/non-root configuration of a meshpoint by:</p> <ul style="list-style-type: none"><li>• Monitoring and ranking the signal strength and path cost of neighboring mesh points.</li><li>• Setting the configuration to:<ul style="list-style-type: none"><li>• <code>non-root</code>: If the link with the shortest path to the cost-root mesh device is a MCX meshpoint link</li><li>• <code>root</code>: If the link with the shortest path to the cost-root mesh device is a non MCX meshpoint link (wired link).</li></ul></li><li>• This requires that the meshpoint device, in the brain car, be configured as the 'cost root' and the 'cost root' meshpoint-device be the I2 gateway to the controller. Use the <code>root-select &gt; cost-root</code> command to configure a meshpoint-device as 'cost-root'.</li><li>• Using signal strength of neighboring meshpoint as the sole metric to determine the next mesh hop to the root.</li><li>• Loop detection with both meshpoints in a car select non-root and form a mesh link with the same root</li></ul> |
| <code>select-method auto-proximity</code> | Enables dynamic root selection using meshpoint proximity. When <code>auto-proximity</code> is selected, root selection is based on signal strength of candidate roots.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

### Examples

```
nx9500-6C8809(config-profile-testAP8432-meshpoint-test)#root select-method auto-mint
nx9500-6C8809(config-profile-testAP8432-meshpoint-test)#show context
meshpoint-device test
 name test
 root select-method auto-mint
 preferred root 22-33-44-55-66-77
```

```

 preferred neighbor 11-22-33-44-55-66
 preferred interface 5GHz
 monitor critical-resource action no-root
nx9500-6C8809(config-profile-testAP8432-meshpoint-test)#
ap8432-070235(config-device-74-67-F7-07-02-35-meshpoint-test)#root select-method auto-mint
ap8432-070235(config-device-74-67-F7-07-02-35-meshpoint-test)#show context
 meshpoint-device test
 root select-method auto-mint
ap8432-070235(config-device-74-67-F7-07-02-35-meshpoint-test)#

```

## Related Commands

|                                                        |                                                                                                                                         |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <code>no (meshpoint-device-config)</code> on page 1800 | Removes the configuration of this meshpoint device as a root meshpoint. Also allows you to disable dynamic mesh selection (if enabled). |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|

*no (meshpoint-device-config)*

Negates the commands for a meshpoint device or resets values to default

### Supported in the following platforms:

- Access Points — AP 6522, AP 6532, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7632, AP 7662, AP 8432, AP 8533

### Syntax

```

no [acs|exclude|hysteresis|monitor|path-method|preferred|root|root-select]
no acs [channel-hold-time|channel-switch-delta|channel-width|ocs-duration|
ocs-frequency|path-min|path-threshold|preferred-interface-tolerance-period|
preferred-radio-interface|priority-meshpoint|sample-count|snr-delta|
signal-threshold|tolerance-period] [2.4GHZ|5GHz]
no exclude wired-peer mint-level-1
no hysteresis [min-threshold|period|root-sel-snr-delta|snr-delta]
no monitor [critical-resource|primary-port-link-loss]
no [path-method|root {select-method}]
no root-select cost-root
no preferred [interface|root|neighbor]

```

### Parameters

no <PARAMETERS>

|                 |                                                                                             |
|-----------------|---------------------------------------------------------------------------------------------|
| no <PARAMETERS> | Removes or reverts this meshpoint device settings to default based on the parameters passed |
|-----------------|---------------------------------------------------------------------------------------------|

### Examples

```

nx9500-6C8809(config-profile-testAP8432-meshpoint-test)#show context
 meshpoint-device test
 name test
 root
 preferred root 22-33-44-55-66-77
 preferred neighbor 11-22-33-44-55-66
 preferred interface 5GHz

```

---

```
monitor critical-resource action no-root
nx9500-6C8809(config-profile-testAP8432-meshpoint-test)#
nx9500-6C8809(config-profile-testAP8432-meshpoint-test))#no monitor critical-resource
nx9500-6C8809(config-profile-testAP8432-meshpoint-test)#no preferred neighbor
nx9500-6C8809(config-profile-testAP8432-meshpoint-test)#no root
nx9500-6C8809(config-profile-testAP8432-meshpoint-test)#no preferred interface
nx9500-6C8809(config-profile-testAP8432-meshpoint-test)#show context
meshpoint-device test
 name test
 no root
 preferred root 22-33-44-55-66-77
nx9500-6C8809(config-profile-testAP8432-meshpoint-test)#
```

# PASSPOINT POLICY

## PASSPOINT POLICY

---

A passpoint policy provides an interoperable platform for streamlining Wi-Fi access to access points deployed as public hotspots. Passpoint is supported across a wide range of wireless network deployment scenarios and client devices. Passpoint makes connecting to Wi-Fi networks easier by authenticating the user with an account based on an existing relationship, such as the user's mobile carrier or broadband ISP.

To migrate to the passpoint policy configuration mode, use the following command:

```
<DEVICE>(config)#passpoint-policy <POLICY-NAME>
rfs4000-229D58(config)#passpoint-policy test
rfs4000-229D58(config-passpoint-policy-test)#
rfs4000-229D58(config-passpoint-policy-test)#?
Passpoint Policy Mode commands:
 3gpp Configure a 3gpp plmn (public land mobile network) id
 access-network-type Set the access network type for the hotspot
 connection-capability Configure the connection capability for the hotspot
 domain-name Add a domain-name for the hotspot
 hessid Set a homogeneous ESSID value for the hotspot
 internet Advertise the hotspot having internet access
 ip-address-type Configure the advertised ip-address-type
 nai-realm Configure a NAI realm for the hotspot
 net-auth-type Add a network authentication type to the hotspot
 no Negate a command or set its defaults
 operator Add configuration related to the operator of the
 hotspot
 osu Online signup
 roam-consortium Add a roam consortium for the hotspot
 venue Set the venue parameters of the hotspot
 wan-metrics Set the wan-metrics of the hotspot

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

rfs4000-229D58(config-passpoint-policy-test)#
```

### passpoint-policy

The following table summarizes the Passpoint Policy configuration mode commands:

**Table 64: Passpoint-Policy Config Mode Commands**

| Command                                            | Description                                                                                        |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------|
| <a href="#">3gpp</a> on page 1803                  | Configures a 3gpp (3rd Generation Partnership Project) PLMN (Public Land Mobile Network) ID        |
| <a href="#">access-network-type</a> on page 1804   | Configures the access network type element in this hotspot                                         |
| <a href="#">connection-capability</a> on page 1805 | Configures the connection capability element in this passpoint policy                              |
| <a href="#">domain-name</a> on page 1807           | Configures the RF Domains to which this hotspot is applicable                                      |
| <a href="#">hessid</a> on page 1807                | Configures the HESSID (Homogeneous Extended Service Set Identifier) for a specified hotspot zone   |
| <a href="#">internet</a> on page 1808              | Advertises the availability of Internet access in this hotspot                                     |
| <a href="#">ip-address-type</a> on page 1809       | Advertises the IP address type used in this hotspot.                                               |
| <a href="#">nai-realm</a> on page 1810             | Configures a NAI (Network Access Identifier) realm name and enters its configuration mode          |
| <a href="#">net-auth-type</a> on page 1813         | Configures the network authentication type used in this hotspot                                    |
| <a href="#">operator</a> on page 1814              | Configures the operator friendly name for this hotspot                                             |
| <a href="#">osu</a> on page 1815                   | Configures an OSU (online sign up) SSID/provider and enters its configuration mode                 |
| <a href="#">roam-consortium</a> on page 1822       | Configures the list of Roaming Consortium OIs (Organization Identifiers) supported on this hotspot |
| <a href="#">venue</a> on page 1823                 | Configures the venue group and type for this passpoint policy                                      |
| <a href="#">wan-metrics</a> on page 1828           | Configures the WAN performance metrics for this hotspot                                            |
| <a href="#">no</a> on page 1829                    | Removes or reverts passpoint policy configuration                                                  |



**Note**

The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore ( \_ ) character. In other words, the name of a device cannot contain an underscore.



**Note**

For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see [COMMON COMMANDS](#).

*3gpp*

Configures a 3GPP (3rd Generation Partnership Project) PLMN (Public Land Mobile Network) information. The 3GPP PLMN information is a combination of the MCC (Mobile Country Code) and MNC (Mobile Network Code). This MCC and MNC combination uniquely identifies a cellular operator. For example, Telstar Corporation Ltd. in Australia is identified by MCC 505 and MNC 001.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
3gpp mcc <MOBILE-COUNTRY-CODE> mnc <MOBILE-NETWORK-CODE> {description <LINE>}
```

### Parameters

```
3gpp mcc <MOBILE-COUNTRY-CODE> mnc <MOBILE-NETWORK-CODE> {description <LINE>}
```

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3gpp                      | Configures the 3GPP PLMN information that is returned in response to an ANQP query                                                                                                                                                                                                                                                                                                                                                                                                         |
| mcc <MOBILE-COUNTRY-CODE> | Specifies the MCC. The MCC is a two or three digit decimal value. For example, the MCC for Australia is 505.                                                                                                                                                                                                                                                                                                                                                                               |
| mnc <MOBILE-NETWORK-CODE> | Specifies the MNC. The MNC is a two or three decimal value used in combination with the MCC to uniquely identify a mobile network operator. The MNC and MCC combination (also known as the MCC/MNC tuple) forms the first five or six digits of the IMSI's (International Mobile Subscriber Identity).<br><br><b>Note:</b> If the MCC and MNC values are not configured, the hotspot will not return the element in an ANQP capability request and ignores any ANQP query for the element. |
| description <LINE>        | Optional. Configures a description that uniquely identifies this PLMN. Provide a description not exceeding 64 characters in length.                                                                                                                                                                                                                                                                                                                                                        |

### Examples

```
rf4000-229D58(config-passpoint-policy-test)#3gpp mcc 505 mnc 14
rf4000-229D58(config-passpoint-policy-test)#3gpp mcc 310 mnc 970
rf4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 3gpp mcc 310 mnc 970
 3gpp mcc 505 mnc 14
rf4000-229D58(config-passpoint-policy-test)#
```

### Related Commands

|    |                                                                                    |
|----|------------------------------------------------------------------------------------|
| no | Removes the specified 3gpp PLMN information and its corresponding MCC/MNC settings |
|----|------------------------------------------------------------------------------------|

### access-network-type

Configures the access network type for this hotspot. The beacons and probe responses communicate the type of hotspot (public, private, guest-use, emergency, etc.) to clients seeking access.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000



## Syntax

```
access-network-type [chargeable-public|emergency-services|experimental|free-public|
personal-device|private|private-guest|wildcard]
```

## Parameters

```
access-network-type [chargeable-public|emergency-services|experimental|free-public|
personal-device|private|private-guest|wildcard]
```

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| access-network-type | Select the access network type for this hotspot. The options are: <ul style="list-style-type: none"><li>• chargeable-public – The network type is a chargeable public network.</li><li>• emergency-services – The network is used to provide emergency services only.</li><li>• experimental – The network is used for test or experimental purposes only.</li><li>• free-public – The network type is a free public.</li><li>• personal-device – The network is used for personal devices only.</li><li>• private – The network is a private network.</li><li>• private-guest – The network is a private network with guest access (default setting).</li><li>• wildcard – Includes all access network types.</li></ul> |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Note:** If the network type is set to chargeable-public, probe responses advertise this hotspot as a chargeable-public hotspot.

## Examples

```
rfs4000-229D58(config-passpoint-policy-test)#access-network-type chargeable-public
rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 access-network-type chargeable-public
 3gpp mcc 310 mnc 970
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

## Related Commands

|    |                                                              |
|----|--------------------------------------------------------------|
| no | Reverts to the default access network type setting (private) |
|----|--------------------------------------------------------------|

## *connection-capability*

Configures the connection capability element in this passpoint policy. When configured, it communicates which ports are open or closed on the Hotspot, in response to an ANQP query.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
connection-capability [ftp|http|icmp|ip-protocol|ipsec-vpn|pptp-vpn|sip|ssh|tls-vpn]
connection-capability [ftp|http|icmp|ipsec-vpn|pptp-vpn|sip|ssh|tls-vpn] [closed|open|
unknown]
connection-capability ip-protocol <0-255> port <0-65535> [closed|open|unknown]
```

## Parameters

connection-capability [ftp|http|icmp|ip-protocol|ipsec-vpn|pptp-vpn|sip|ssh|tls-vpn]

|                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| connection-capability                      | Configures the connection capability element in this passpoint policy                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| ftp                                        | Specifies the protocol type as FTP. Configures TCP port 20.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| http                                       | Specifies the protocol type as HTTP. Configures TCP port 80.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| icmp                                       | Specifies the protocol type as ICMP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| ipsec-vpn                                  | Specifies the protocol type as IPSEC VPN. Configures ESP and UDP ports 500 and 4500.                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| pptp-vpn                                   | Specifies the protocol type as PPTP VPN. Configures TCP port 1723.                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| sip                                        | Specifies the protocol type as SIP. Configures TCP port 5060 and UDP port 5060.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| ssh                                        | Specifies the protocol type as SSH. Configures TCP port 20                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| tls-vpn                                    | Specifies the protocol type as TLS VPN. Configures TCP port 443.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| port <0-65535><br>[closed open]<br>unknown | <p>After specifying the protocol type, specify the port (associated with the selected protocol) and its status.</p> <ul style="list-style-type: none"> <li>closed – Specifies that the port(s) is/are closed</li> <li>open – Specifies that the port(s) is/are open</li> <li>unknown – Specifies that the port(s) status is not known</li> </ul> <p><b>Note:</b> When the connection capability element is not configured, the hotspot does not return the element in an ANQP capability request and ignores any ANQP query for the element.</p> |

connection-capability ip-protocol <0-255> port <0-65535> [closed|open|unknown]

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| connection-capability                       | Configures the connection capability element in this passpoint policy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| ip-protocol<br><0-255>                      | Identifies the IP protocol by the protocol's number. For example, for SMP (simple message protocol) specify 121.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| port <0-65535><br>[closed open <br>unknown] | <p>After specifying the IP protocol type, specify the port number.</p> <ul style="list-style-type: none"> <li>port &lt;0-65535&gt; – Select a port for the IP protocol identified.</li> </ul> <p>After specifying the port number, specify the port status.</p> <ul style="list-style-type: none"> <li>closed – Specifies that the port(s) is/are closed</li> <li>open – Specifies that the port(s) is/are open</li> <li>unknown – Specifies that the port(s) status is not known</li> </ul> <p><b>Note:</b> When the connection capability element is not configured, the hotspot does not return the element in an ANQP capability request and ignores any ANQP query for the element.</p> |

## Examples

```
rfs4000-229D58(config-passpoint-policy-test)#connection-capability 1 ip-protocol 2 port 10
closed
rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
access-network-type chargeable-public
connection-capability ip-protocol 2 port 10 closed
3gpp mcc 310 mnc 970
3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

## Related Commands

**no** Removes the configured connection capability element on the passpoint policy

### *domain-name*

Configures the RF Domain(s) that are returned in response to an ANQP query

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

domain-name <DOMAIN-NAME>

#### Parameters

domain-name <DOMAIN-NAME>

domain-name <DOMAIN-NAME> Specify the RF Domain name

**Note:** An hotspot can be applied across multiple RF Domains.

#### Examples

```
rfs4000-229D58(config-passpoint-policy-test)#domain-name TechPubs
rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 access-network-type chargeable-public
 connection-capability ip-protocol 2 port 10 closed
 domain-name TechPubs
 3gpp mcc 310 mnc 970
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

## Related Commands

**no** Removes the RF Domain mapped to this passpoint policy

### *hessid*

Configures the HESSID (Homogeneous Extended Service Set Identifier) for the hotspot. The HESSID uniquely identifies a hotspot provider within a zone. This is essential in zones (such as an airport or shopping mall) having multiple hotspot service providers with overlapping coverage.

An HESSID is a 6 (six) byte identifier that uniquely identifies a set of APs belonging to the same network and exhibiting same network behaviour. It is the BSSID of one of the devices (AP) in the zone. When not configured, the radio's BSSID is used as the HESSID.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
hessid <MAC>
```

### Parameters

```
hessid <MAC>
```

|              |                                                                     |
|--------------|---------------------------------------------------------------------|
| hessid <MAC> | Specify a unique 6 (six) byte identifier for this passpoint policy. |
|--------------|---------------------------------------------------------------------|

### Examples

```
rfs4000-229D58(config-passpoint-policy-test)#hessid 00-23-68-88-0D-A7
rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 access-network-type chargeable-public
 connection-capability ip-protocol 2 port 10 closed
 domain-name TechPubs
 hessid 00-23-68-88-0D-A7
 3gpp mcc 310 mnc 970
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

### Related Commands

|    |                                                                                                      |
|----|------------------------------------------------------------------------------------------------------|
| no | Removes the HESSID configured with this passpoint policy and reverts back to using the radio's BSSID |
|----|------------------------------------------------------------------------------------------------------|

### *internet*

Advertises the availability of Internet access on this hotspot. The Internet bit in the hotspot's beacon and probe responses indicates if Internet access is available or not. By default this feature is enabled.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
internet
```

### Parameters

None

### Examples

```
rfs4000-229D58(config-passpoint-policy-test)#internet
rfs4000-229D58(config-passpoint-policy-test)#
```

## Related Commands

|                 |                                                  |
|-----------------|--------------------------------------------------|
| <code>no</code> | Removes Internet access on this passpoint policy |
|-----------------|--------------------------------------------------|

### *ip-address-type*

Advertises the IP address type used in this hotspot. This information is returned in response to ANQP queries.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
ip-address-type [ipv4 | ipv6]
ip-address-type ipv4 [double-nat | not-available | port-restricted | port-restricted-double-nat |
port-restricted-single-nat | public | single-nat | unknown]
ip-address-type ipv6 [available | not-available | unknown]
```

#### Parameters

```
ip-address-type ipv4 [double-nat | not-available | port-restricted | port-restricted-double-nat |
port-restricted-single-nat | public | single-nat | unknown]
```

|                                         |                                                                                   |
|-----------------------------------------|-----------------------------------------------------------------------------------|
| <code>ip-address-type ipv4</code>       | Configures the IPv4 address type availability information                         |
| <code>double-nat</code>                 | Specifies double NATed private IPv4 address is available                          |
| <code>not-available</code>              | Specifies IPv4 address is not available                                           |
| <code>port-restricted</code>            | Specifies port-restricted IPV4 address is available                               |
| <code>port-restricted-double-nat</code> | Specifies port-restricted IPv4 address and double NATed IPv4 address is available |
| <code>port-restricted-single-nat</code> | Specifies port-restricted IPv4 address and single NATed IPv4 address is available |
| <code>public</code>                     | Specifies public IPv4 address is available                                        |
| <code>single-nat</code>                 | Specifies single NATed IPv4 address is available                                  |
| <code>unknown</code>                    | Specifies no information configured regarding the IPv4 address availability       |

```
ip-address-type ipv6 [available | not-available | unknown]
```

|                                   |                                                                             |
|-----------------------------------|-----------------------------------------------------------------------------|
| <code>ip-address-type ipv6</code> | Configures the IPv6 address type availability information                   |
| <code>available</code>            | Specifies IPv6 address is available                                         |
| <code>not-available</code>        | Specifies IPv6 address is not available                                     |
| <code>unknown</code>              | Specifies no information configured regarding the IPv6 address availability |

#### Examples

```
rfs4000-229D58(config-passpoint-policy-test)#ip-address-type ipv6 available
rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 access-network-type chargeable-public
```

```

connection-capability ip-protocol 2 port 10 closed
domain-name TechPubs
hessid 00-23-68-88-0D-A7
ip-address-type ipv6 available
3gpp mcc 310 mnc 970
3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#

```

## Related Commands

**no** Removes the IP address type configured for this passpoint policy

### *nai-realm*

Configures a NAI (Network Access Identifier) realm name and enters its configuration mode

The NAI is the user identity submitted by the hotspot requesting client during authentication. The standard syntax is user@realm. NAI is frequently used when roaming, to identify the user and assist in routing an authentication request to the user’s authentication server. The realm name is often the domain name of the service provider.

You can configure a list of NAI realm names of service providers operating within a specific hotspot zone. This NAI realm name list is presented in ANQP response to a NAI realm and NAI home realm query.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
nai-realm <NAI-REALM-NAME>
```

### Parameters

```
nai-realm <NAI-REALM-NAME>
```

|                            |                                                                                                                                                                                                                                                                                     |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| nai-realm <NAI-REALM-NAME> | <p>Configures the NAI realm name for this passpoint policy</p> <ul style="list-style-type: none"> <li>• &lt;NAI-REALM-NAME&gt; – Specify the NAI realm name (32 characters maximum) for this passpoint policy. You can provide multiple names delimited by a semi colon.</li> </ul> |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```

nx9500-6C8809(config-passpoint-policy-test)#nai-realm example
nx9500-6C8809(config-passpoint-policy-test-nai-realm-example)#?
Passpoint NAI Realm Mode commands:
 eap-method Set an eap method
 no Negate a command or set its defaults

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode

```

```

help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

```

```

nx9500-6C8809(config-passpoint-policy-test-nai-realm-example)#
nx9500-6C8809(config-passpoint-policy-test)#show context
passpoint-policy test
access-network-type chargeable-public
connection-capability ip-protocol 2 port 10 closed
nai-realm example
3gpp mcc 505 mnc 14
nx9500-6C8809(config-passpoint-policy-test)#

```

The following table summarizes NAI realm configuration mode commands.

**Table 65: NAI-Realm-Config-Mode Commands**

| Command                 | Description                                                                                                                   |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <code>eap-method</code> | Specifies the EAP authentication mechanisms supported by each of the service providers associated with this passpoint policy. |

#### Related Commands

|                 |                                                                 |
|-----------------|-----------------------------------------------------------------|
| <code>no</code> | Removes the NAI realm name configured for this passpoint policy |
|-----------------|-----------------------------------------------------------------|

### eap-method

Specifies the EAP authentication mechanisms supported by each of the service providers associated with this passpoint policy.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```

eap-method <1-10> [<1-255>|fast|gtc|identity|ikev2|ms-auth|mschapv2|otp|peap|psk|rsa-
public-key|
sim|tls|ttls] auth-param [credential|expanded-eap|expanded-inner-eap|inner-eap|non-eap-
inner|
tunn-eap-credential|vendor] [cert|hw-token|nfc-secure-elem|none|sim|soft-token|username-
password|usim|
vendor]

```

#### Parameters

```

eap-method <1-10> [<1-255>|fast|gtc|identity|ikev2|ms-auth|mschapv2|otp|peap|psk|rsa-
public-key|
sim|tls|ttls] auth-param [credential|expanded-eap|expanded-inner-eap|inner-eap|non-eap-
inner|
tunn-eap-credential|vendor] [cert|hw-token|nfc-secure-elem|none|sim|soft-token|username-
password|usim|
vendor]

```

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| eap-method<br><1-10> | <p>Selects the EAP authentication method used and assigns it an index number</p> <ul style="list-style-type: none"> <li>• &lt;1-10&gt; - Specify an identifier for this EAP method from 1 - 10. The Index specified here is applied to this hotspot's EAP credential exchange and verification sessions. NAIs are often user identifiers in the EAP authentication protocol.</li> </ul> <p>A maximum of 10 (ten) authentication methods can be specified for every NAI realm. After creating the EAP authentication method, specify the associated authentication mechanisms (method types).</p> |
| <1-255>              | <p>Identifies the EAP authentication method type from the corresponding IANA (Internet Assigned Numbers Authority) number</p> <ul style="list-style-type: none"> <li>• &lt;1-255&gt; - Specify the IANA identity number for the authentication protocol from 1 - 255.</li> </ul>                                                                                                                                                                                                                                                                                                                 |
| fast                 | Specifies the EAP authentication method type as FAST (Flexible Authentication via Secure Tunneling)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| gtc                  | Specifies the EAP authentication method type as GTC (Generic Token Card)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| identity             | Specifies the EAP authentication method type as Identification                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| ikev2                | Specifies the EAP authentication method type as IKEv2 (Internet Key Exchange Protocol version 2)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| ms-auth              | Specifies the EAP authentication method type as MS-Auth (Microsoft Authentication)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| mschapv2             | Specifies the EAP authentication method type as MSCHAPv2 (Microsoft Challenge Handshake Authentication Protocol Version 2)                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| opt                  | Specifies the EAP authentication method type as OTP (One Time Password)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| peap                 | Specifies the EAP authentication method type as PEAP (Protected Extensible Authentication Protocol)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| psk                  | Specifies the EAP authentication method type as PSK (Pre-shared Key)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| rsa-public-key       | Specifies the EAP authentication method type as RSA public key protocol                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| sim                  | Specifies the EAP authentication method type as GSM SIM (Subscriber Identity Module)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| tls                  | Specifies the EAP authentication method type as TLS (Transport Layer Security)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| ttls                 | Specifies the EAP authentication method type as TTLS (Tunneled Transport Layer Security)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |



|                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| auth-param                                                                        | After specifying the EAP authentication method type, specify the authentication parameters. These parameters depend on the EAP authentication mechanism selected.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| [cert hw-token nfc-secure-elem none sim soft-token username-password usim vendor] | <p>The following parameters are common to all the above authentication parameters:</p> <ul style="list-style-type: none"> <li>• cert – Certificate</li> <li>• hw-token – Hardware token</li> <li>• nfc-secure-elem – NFC secure element</li> <li>• none – No credential</li> <li>• sim – Subscriber identity module</li> <li>• soft-token – Soft token</li> <li>• username-password – Username and password</li> <li>• usim – Universal subscriber identity module</li> <li>• vendor – Vendor specific credential</li> </ul> <p>If setting the authentication type to either <b>non-eap-inner</b>, <b>inner-eap-credential</b>, or <b>tunneleap-credential</b>, define an authentication value that must be shared with the EAP credential validation server resource.</p> <p>If setting the authentication type to either <b>expanded-eap</b> or <b>expanded-inner-eap</b>, set a required authentication vendor ID that must match the one utilized by the EAP server resource. The ID must be 6 characters in length.</p> <p>If required, enter a 2 - 510 character vendor-specific authentication data required for the selected authentication type. Enter the value in the a-FA -FO-9 format.</p> <p>Provide an authentication vendor type, used exclusively for the <b>expanded-eap</b> or <b>expanded-inner-eap</b> authentication types. The vendor type must be 8 characters in length.</p> |

### Examples

```

nx9500-6C8809(config-passpoint-policy-test-nai-realm-example)#eap-method 1 ttls auth-param
vendor hex 00001E
nx9500-6C8809(config-passpoint-policy-test-nai-realm-example)#eap-method 2 rsa-public-key
auth-param credential cert
nx9500-6C8809(config-passpoint-policy-test-nai-realm-example)#show context
nai-realm example
 eap-method 1 ttls auth-param vendor hex 00001E
 eap-method 2 rsa-public-key auth-param credential cert
nx9500-6C8809(config-passpoint-policy-test-nai-realm-example)#exit
nx9500-6C8809(config-passpoint-policy-test)#show context
passpoint-policy test
 access-network-type chargeable-public
 connection-capability ip-protocol 2 port 10 closed
 nai-realm example
 eap-method 1 ttls auth-param vendor hex 00001E
 eap-method 2 rsa-public-key auth-param credential cert
 3gpp mcc 505 mnc 14
nx9500-6C8809(config-passpoint-policy-test)#

```

### *net-auth-type*

Configures the network authentication type used in this hotspot. The details configured are returned in response to an ANQP query. Use this option to specify how W-iFi connection attempts are authenticated and validated using a dedicated redirection URL resource.

#### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000

- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
net-auth-type [accept-terms|dns-redirect|http-redirect|online-enroll] {url <URL>}
```

### Parameters

```
net-auth-type [accept-terms|dns-redirect|http-redirect|online-enroll] {url <URL>}
```

|               |                                                                                                                                                                                           |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| net-auth-type | Specifies the network authentication type used with this passpoint policy. The options are: <b>accept-terms</b> , <b>dns-redirect</b> , <b>http-redirect</b> , and <b>online-enroll</b> . |
| accept-terms  | Enables user acceptance of terms and conditions                                                                                                                                           |
| dns-redirect  | Enables DNS redirection of user                                                                                                                                                           |
| http-redirect | Enables HTTP redirection of user                                                                                                                                                          |
| online-enroll | Enables online user enrolment                                                                                                                                                             |
| url <URL>     | Optional. Specify the location for each of above network authentication types.                                                                                                            |

### Examples

```
nx9500-6C8809(config-passpoint-policy-test)#net-auth-type accept-terms url www.test.com
nx9500-6C8809(config-passpoint-policy-test)#show context
passpoint-policy test
 access-network-type chargeable-public
 connection-capability ip-protocol 2 port 10 closed
 nai-realm example
 eap-method 1 ttls auth-param vendor hex 00001E
 eap-method 2 rsa-public-key auth-param credential cert
 net-auth-type accept-terms url www.test.com
 3gpp mcc 505 mnc 14
nx9500-6C8809(config-passpoint-policy-test)#
```

### Related Commands

|    |                                                                               |
|----|-------------------------------------------------------------------------------|
| no | Removes the network authentication type configured with this passpoint policy |
|----|-------------------------------------------------------------------------------|

### operator

Configures a unique name of the administrator or operator responsible for the configuration and management of the hotspot. The name can be configured in English or in any language other than English. When the name is specified in English, the system allows an ASCII input. If using a language other than English, first specify the ISO-639 language code, and then specify the name as an hexadecimal code.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
operator name [<OPERATOR-NAME>|iso-lang <ISO-639-LANG-CODE> <OPERATOR-NAME>]
```

## Parameters

`operator name [<OPERATOR-NAME>|iso-lang <ISO-639-LANG-CODE> <OPERATOR-NAME>]`

|                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>name &lt;OPERATOR-NAME&gt;</code>                                   | Configures the operator's name in English <ul style="list-style-type: none"><li><code>&lt;OPERATOR-NAME&gt;</code> - Specify the operator name in ASCII format. The name cannot exceed 252 characters.</li></ul>                                                                                                                                                                                                                          |
| <code>iso-lang &lt;ISO-639-LANG-CODE&gt;<br/>&lt;OPERATOR-NAME&gt;</code> | Configures the operator's name in any language other than English <ul style="list-style-type: none"><li><code>iso-lang &lt;ISO-639-LANG-CODE&gt;</code> - Specify the three-character ISO-14962-1997 encoded string defining the language used in the Code field. For example, chi or spa.</li><li><code>&lt;OPERATOR-NAME&gt;</code> - Specify the operator name in Hexadecimal format. The name cannot exceed 252 characters.</li></ul> |

## Examples

```
nx9500-6C8809(config-passpoint-policy-test)#operator name exampleoperator
nx9500-6C8809(config-passpoint-policy-test)#show context
passpoint-policy test
 access-network-type chargeable-public
 connection-capability ip-protocol 2 port 10 closed
 nai-realm example
 eap-method 1 ttls auth-param vendor hex 00001E
 eap-method 2 rsa-public-key auth-param credential cert
 net-auth-type accept-terms url www.test.com
 operator name exampleoperator
 3gpp mcc 505 mnc 14
nx9500-6C8809(config-passpoint-policy-test)#
```

## Related Commands

|                 |                                                                  |
|-----------------|------------------------------------------------------------------|
| <code>no</code> | Removes the operator's name configured for this passpoint policy |
|-----------------|------------------------------------------------------------------|

## OSU

Adds an osu (online sign up) SSID (WLAN)/OSU provider and enters its configuration mode

WiNG managed clients can use OSU for registration and credential provisioning to obtain hotspot network access. Service providers have an OSU AAA server and CA (certificate authority). For a client and hotspot to trust one another, the OSU server holds a certificate signed by a CA whose root certificate is issued by a CA authorized by the Wi-Fi Alliance, and CA certificates are installed on the client device. A CA performs four functions:

- Issues certificates (creates and signs)
- Maintains certificate status information and issues CRLs (certificate revocation lists)
- Publishes current (non-expired) certificates and CRLs
- Maintains status archives for the expired or revoked certificates it has issued

Passpoint certificates are governed by the Hotspot 2.0 OSU Certificate Policy Specification. An OSU server certificate should be obtained from any of the CAs authorized by the Wi-Fi Alliance.

Once an OSU provider is selected, the client connects to the OSU WLAN (Open or OSEN). It then triggers an HTTPS connection to the OSU server, which was received with the OSU providers list. The client validates the server certificate to ensure it's a trusted OSU server. The client is then prompted to complete an online registration through their browser. When the client has a valid credential for the

hotspot 2.0 WLAN, it disassociates from the OSU WLAN and connects to the hotspot 2.0 WLAN using standard ANQP mechanisms.

**Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

**Syntax**

```
osu [provider <PASSPOINT-OSU-PROVIDER>|ssid <SSID>]
```

**Parameters**

```
osu [provider <PASSPOINT-OSU-PROVIDER>|ssid <SSID>]
```

|                                   |                                                                                                                                                                                                                                                                                                       |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| osu                               | Use this command to configure an OSU SSID/OSU provider.                                                                                                                                                                                                                                               |
| provider <PASSPOINT-OSU-PROVIDER> | Creates an OSU provider for this passpoint and enters its configuration mode <ul style="list-style-type: none"> <li>• &lt;PASSPOINT-OSU-PROVIDER&gt; - Specify an identification for this OSU passpoint provider serving as an online sign up identifier. Should not exceed 32 characters.</li> </ul> |
| ssid <SSID>                       | Configures an OSU WLAN's SSID. This is the open authentication SSID that a user can use to obtain credentials for the passpoint SSID. <ul style="list-style-type: none"> <li>• &lt;SSID&gt; - Specify the SSID.</li> </ul>                                                                            |

**Examples**

```
nx9500-6C8809(config-passpoint-policy-test)#osu provider test
nx9500-6C8809(config-passpoint-policy-test-osu-provider-test)#?
Passpoint OSU Provider Mode commands:
 description Configure the English description of the online signup provider
 icon Add an icon for the online signup provider
 method Specify the online signup method supported by provider
 nai Configure the NAI for the online signup provider
 name Configure the english name of the online signup provider
 no Negate a command or set its defaults
 server-url Configure the signup url for the online signup provider

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-passpoint-policy-test-osu-provider-test)#
```

The following table summarizes NAI realm configuration mode commands:

**Table 66:**

| Command                                                    | Description                                                        |
|------------------------------------------------------------|--------------------------------------------------------------------|
| <a href="#">description (osu-config-mode)</a> on page 1817 | Configures the OSU provider's description                          |
| <a href="#">icon (osu-config-mode)</a> on page 1818        | Adds the OSU provider's icon                                       |
| <a href="#">method (osu-config-mode)</a> on page 1819      | Configures the open sign up methods available on this OSU provider |
| <a href="#">nai (osu-config-mode)</a> on page 1820         | Configures the OSU provider's NAI                                  |
| <a href="#">name (osu-config-mode)</a> on page 1820        | Configures the OSU provider's name                                 |
| <a href="#">server-url (osu-config-mode)</a> on page 1821  | Configures the OSU provider server's URL                           |
| <a href="#">no (osu-config-mode)</a> on page 1822          | Removes the settings configured for this OSU provider              |

**Related Commands**

|                                 |                                                                     |
|---------------------------------|---------------------------------------------------------------------|
| <a href="#">no</a> on page 1829 | Removes the OSU WLAN/provider configured with this passpoint policy |
|---------------------------------|---------------------------------------------------------------------|

**description (osu-config-mode)**

Configures the OSU SSID/provider's description. This value is returned in the ANQP OSU providers list.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
description [<DESCRIPTION>|iso-lang <ISO-LANG-CODE> <DESCRIPTION>]
```

## Parameters

```
description [<DESCRIPTION>|iso-lang <ISO-LANG-CODE> <DESCRIPTION>]
```

|                                           |                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <DESCRIPTION>                             | Configures the OSU provider's description in English. It should not exceed 253 characters in length. <ul style="list-style-type: none"> <li>• &lt;DESCRIPTION&gt; - Specify the description. By default the system configures the name in English.</li> </ul> <p><b>Note:</b> If configuring description in any language other than English, use the 'iso-lang' option to provide the language code.</p> |
| iso-lang <ISO-LANG-CODE><br><DESCRIPTION> | Identifies the language by its ISO 639 language code (for example, 'chi-chinese' or 'spa-spanish'). By default the language is set to English. If specifying the description in any language other than English, specify the ISO language code. <ul style="list-style-type: none"> <li>• &lt;DESCRIPTION&gt; - Specify the description in hexadecimal code.</li> </ul>                                   |

## Examples

```
nx9500-6C8809(config-passpoint-policy-test-osu-provider-test)#description "OSU created for testing purposes."
nx9500-6C8809(config-passpoint-policy-test-osu-provider-test)#show context
osu provider test
```

```
description "OSU created for testing purposes."
nx9500-6C8809(config-passpoint-policy-test-osu-provider-test)#
```

#### Related Commands

|                                   |                                                      |
|-----------------------------------|------------------------------------------------------|
| <code>no (osu-config-mode)</code> | Removes this OSU provider's description on page 1822 |
|-----------------------------------|------------------------------------------------------|

### icon (osu-config-mode)

Adds the OSU provider's icon. This value is returned in the ANQP OSU providers list.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
icon iso-lang <ISO-LANG-CODE> width <0-65535> height <0-65535> mime-type <FILE-MIME-TYPE>
file [<IMAGE-FILE-NAME/PATH>|<FILE-NAME>]
```

#### Parameters

```
icon iso-lang <ISO-LANG-CODE> width <0-65535> height <0-65535> mime-type <FILE-MIME-TYPE>
file [<IMAGE-FILE-NAME/PATH>|<FILE-NAME>]
```

|                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>icon iso-lang &lt;ISO-LANG-CODE&gt;</code>                   | Configures an icon representing the OSU provider <ul style="list-style-type: none"><li>• <code>iso-lang &lt;ISO-LANG-CODE&gt;</code> - Identifies the language by its ISO 639 language code (for example, 'chi-chinese' or 'spa-spanish'). By default the language is set to English. If specifying the image file name and path in any language other than English, specify the ISO language code.</li></ul> |
| <code>width &lt;0-65535&gt;</code>                                 | Configures the icon's width in pixels <ul style="list-style-type: none"><li>• <code>&lt;0-65535&gt;</code> - Specify a value from 0 - 65535 pixels.</li></ul>                                                                                                                                                                                                                                                 |
| <code>height &lt;0-65535&gt;</code>                                | Configures the icon's height in pixels <ul style="list-style-type: none"><li>• <code>&lt;0-65535&gt;</code> - Specify a value from 0 - 65535 pixels.</li></ul>                                                                                                                                                                                                                                                |
| <code>mime-type &lt;FILE-MIME-TYPE&gt;</code>                      | Configures a string describing the icon's standard mime type. The MIME associates filename extensions with a MIME type. A MIME enables a fallback on an extension and are frequently used by Web servers. <ul style="list-style-type: none"><li>• <code>&lt;FILE-MIME-TYPE&gt;</code> - Specify the icon's mime type.</li></ul>                                                                               |
| <code>file [&lt;IMAGE-FILE-NAME/PATH&gt; &lt;FILE-NAME&gt;]</code> | Configures the location and name of the image file <ul style="list-style-type: none"><li>• <code>&lt;IMAGE-FILE-NAME/PATH&gt;</code> - Specify the path and filename (255 character maximum). For example, flash:/icon.png</li><li>• <code>&lt;FILE-NAME&gt;</code> - Use this option to specify the filename in the flash:/ directory</li></ul>                                                              |

#### Examples

```
nx9500-6C8809(config-passpoint-policy-test-osu-provider-test)#icon iso-lang eng width 128
height 128 mime-type image/png file falsh:/testicon
nx9500-6C8809(config-passpoint-policy-test-osu-provider-test)#show context
osu provider test
description "OSU created for testing purposes."
```

```
icon iso-lang eng width 128 height 128 mime-type image/png file falsh:/testicon
nx9500-6C8809(config-passpoint-policy-test-osu-provider-test)#
```

#### Related Commands

|                                                   |                                          |
|---------------------------------------------------|------------------------------------------|
| <code>no (osu-config-mode)</code><br>on page 1822 | Removes this OSU provider's icon details |
|---------------------------------------------------|------------------------------------------|

### method (osu-config-mode)

Configures the open sign up methods available on this OSU provider. This value is returned, in the specified order of precedence, in the ANQP OSU providers list.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
method [oma-dm|soap-xml-spp] priority <1-2>
```

#### Parameters

```
method [oma-dm|soap-xml-spp] priority <1-2>
```

|                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>method [oma-dm soap-xml-spp]</code><br><code>priority &lt;1-2&gt;</code> | <p>Configures the online sign up methods supported by this OSU provider</p> <ul style="list-style-type: none"><li>• <code>oma-dm</code> - <code>oma-dm</code> - Configures the OSU method used as OMA (Open Mobile Alliance) device management. The OMA is a standards body developing open standards for mobile clients. OMA is relevant to service providers working across countries (with different languages), operators and mobile terminals. Adherence to OMA is strictly voluntary.</li><li>• <code>soap-xml-spp</code> - Configures the OSU method used as Soap-xml subscription provisioning protocol. The SOAP (simple object access protocol) is a protocol for exchanging structured information in Web services. SOAP uses XML as its message format, and relies on other application layer protocols, like HTTP or SMTP for message negotiation and transmission.<ul style="list-style-type: none"><li>• <code>priority &lt;1-2&gt;</code> - Sets the priority of the specified method. Select a value from 1 - 2. The default is one (1).</li></ul></li></ul> |
|--------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config-passpoint-policy-test-osu-provider-test)#method soap-xml-spp priority
2
nx9500-6C8809(config-passpoint-policy-test-osu-provider-test)#show context
osu provider test
description "OSU created for testing purposes."
icon iso-lang eng width 128 height 128 mime-type image/png file falsh:/testicon
method soap-xml-spp priority 2
nx9500-6C8809(config-passpoint-policy-test-osu-provider-test)#
```

#### Related Commands

|                                                   |                                                                    |
|---------------------------------------------------|--------------------------------------------------------------------|
| <code>no (osu-config-mode)</code><br>on page 1822 | Removes the online sign up methods configured on this OSU provider |
|---------------------------------------------------|--------------------------------------------------------------------|

## nai (osu-config-mode)

Configures the OSU provider's NAI. This value is returned in the ANQP OSU providers list.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
nai <WORD>
```

Parameters

```
nai <WORD>
```

|            |                                                                                                                                                                                                                                                                                                                           |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| nai <WORD> | Configures the OSU provider's NAI <ul style="list-style-type: none"><li>• &lt;WORD&gt; - Specify the NAI. Enter a 255 character maximum NAI to identify the user and assist in routing an authentication request to the authentication server. The realm name is often the domain name of the service provider.</li></ul> |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Examples

```
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#nai test.org
nx9500-6C8809(config-passpoint-policy-test-osu-provider-test)#show context
osu provider test
description "OSU created for testing purposes."
icon iso-lang eng width 128 height 128 mime-type image/png file falsh:/testicon
method soap-xml-spp priority 2
nai test.org
nx9500-6C8809(config-passpoint-policy-test-osu-provider-test)#
```

Related Commands

|                                      |                                 |
|--------------------------------------|---------------------------------|
| no (osu-config-mode)<br>on page 1822 | Removes this OSU provider's NAI |
|--------------------------------------|---------------------------------|

## name (osu-config-mode)

Configures the OSU provider's name. This value is returned in the ANQP OSU providers list.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
name [<NAME>|iso-lang <ISO-LANG-CODE> <NAME>]
```

Parameters

```
name [<NAME>|iso-lang <ISO-LANG-CODE> <NAME>]
```



|                                    |                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <NAME>                             | Configures the OSU provider's name. It should not exceed 253 characters in length. <ul style="list-style-type: none"> <li>&lt;NAME&gt; - Specify the name in ASCII format. By default the system configures the name in English.</li> </ul>                                                                                             |
| iso-lang <ISO-LANG-CODE><br><NAME> | Identifies the language by its ISO 639 language code (for example, 'chinese' or 'spanish'). By default the language is set to English. If specifying the name in any language other than English, specify the ISO language code. <ul style="list-style-type: none"> <li>&lt;NAME&gt; - Specify the name in hexadecimal code.</li> </ul> |

### Examples

```

nx9500-6C8809(config-passpoint-policy-test-osu-provider-test)#name testOSU
nx9500-6C8809(config-passpoint-policy-test-osu-provider-test)#show context
 osu provider test
 name testOSU
 description "OSU created for testing purposes."
 icon iso-lang eng width 128 height 128 mime-type image/png file falsh:/testicon
 method soap-xml-spp priority 2
 nai test.org
nx9500-6C8809(config-passpoint-policy-test-osu-provider-test)#

```

### Related Commands

|                                             |                                  |
|---------------------------------------------|----------------------------------|
| <b>no (osu-config-mode)</b><br>on page 1822 | Removes this OSU provider's name |
|---------------------------------------------|----------------------------------|

## server-url (osu-config-mode)

Configures the OSU provider sign-up server's URL. This value is returned in the ANQP OSU providers list.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
server-url <URL>
```

### Parameters

```
server-url <URL>
```

|                  |                                                                                                                                                                      |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| server-url <URL> | Configures the OSU provider server's URL <ul style="list-style-type: none"> <li>&lt;URL&gt; - Specify the server's url. Should not exceed 255 characters.</li> </ul> |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```

nx9500-6C8809(config-passpoint-policy-test-osu-provider-test)#server-url test.example.com
nx9500-6C8809(config-passpoint-policy-test-osu-provider-test)#show context
 osu provider test
 name testOSU
 description "OSU created for testing purposes."
 icon iso-lang eng width 128 height 128 mime-type image/png file falsh:/testicon
 method soap-xml-spp priority 2
 nai test.org

```

```
server-url test.example.com
nx9500-6C8809(config-passpoint-policy-test-osu-provider-test)#
```

#### Related Commands

|                                   |                                                       |
|-----------------------------------|-------------------------------------------------------|
| <code>no (osu-config-mode)</code> | Removes this OSU provider's server's URL on page 1822 |
|-----------------------------------|-------------------------------------------------------|

### no (osu-config-mode)

Removes the settings configured for this OSU provider. Once removed the information is not included in the ANQP providers list.

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
no [description|icon|method|nai|name|server-url]
no [description|icon|name] {iso-lang <ISO-LANG-CODE>}
no [nai|server-url]
no method [oma-dm|soap-xml-spp]
```

#### Parameters

```
no <PARAMETERS>
```

|                                    |                                                       |
|------------------------------------|-------------------------------------------------------|
| <code>no &lt;PARAMETERS&gt;</code> | Removes the settings configured for this OSU provider |
|------------------------------------|-------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config-passpoint-policy-test-osu-provider-test)#show context
osu provider test
name testOSU
description "OSU created for testing purposes."
icon iso-lang eng width 128 height 128 mime-type image/png file falsh:/testicon
method soap-xml-spp priority 2
nai test.org
server-url test.exampe.com
nx9500-6C8809(config-passpoint-policy-test-osu-provider-test)#
nx9500-6C8809(config-passpoint-policy-test-osu-provider-test)#no description
nx9500-6C8809(config-passpoint-policy-test-osu-provider-test)#no icon iso-lang eng
nx9500-6C8809(config-passpoint-policy-test-osu-provider-test)#show context
osu provider test
name testOSU
method soap-xml-spp priority 2
nai test.org
server-url test.exampe.com
nx9500-6C8809(config-passpoint-policy-test-osu-provider-test)#
```

### roam-consortium

Configures a list of RC (Roaming Consortium) OIs (Organization Identifiers) supported on this hotspot. The beacons and probe responses communicate this Roaming Consortium list to devices. This information enables a device to identify the networks available through this AP.

Each OI identifies a either a group of SSPs (Subscription Service Providers) or a single SSP.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
roam-consortium hex <WORD>
```

### Parameters

```
roam-consortium hex <WORD>
```

|                            |                                                                                                                                                                                                                                |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| roam-consortium hex <WORD> | Adds a Roaming Consortium OI to this hotspot in hexadecimal format <ul style="list-style-type: none"><li>• &lt;WORD&gt; - Specify the Roaming Consortium OI in hexadecimal format (should not exceed 128 characters)</li></ul> |
| hex <WORD>                 | Configures a hexadecimal input <ul style="list-style-type: none"><li>• &lt;WORD&gt; - Specify the Roaming Consortium OI in hexadecimal format (should not exceed 128 characters)</li></ul>                                     |

### Examples

```
nx9500-6C8809(config-passpoint-policy-test)#roam-consortium hex 223344
nx9500-6C8809(config-passpoint-policy-test)#show context
passpoint-policy test
 access-network-type chargeable-public
 connection-capability ip-protocol 2 port 10 closed
 nai-realm example
 eap-method 1 ttls auth-param vendor hex 00001E
 eap-method 2 rsa-public-key auth-param credential cert
 net-auth-type accept-terms url www.test.com
 operator name exampleoperator
 roam-consortium hex 223344
 3gpp mcc 505 mnc 14
 osu ssid test
 osu provider test
 name testOSU
 method soap-xml-spp priority 2
 nai test.org
 server-url test.exampe.com
nx9500-6C8809(config-passpoint-policy-test)#
```

### Related Commands

|           |                                                                       |
|-----------|-----------------------------------------------------------------------|
| <b>no</b> | Removes the Roaming Consortium OIs supported on this passpoint policy |
|-----------|-----------------------------------------------------------------------|

### venue

Configures the venue where this hotspot is located. The hotspot venue configuration informs prospective clients about the hotspot's nature of activity, such as educational, institutional, residential, etc.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
venue [group|name]
venue group [assembly|business|educational|industrial|institutional|mercantile|
outdoor|residential|storage|unspecified|utility-and-misc|vehicular] type
venue name [<VENUE-NAME>|iso-lang]
venue name <VENUE-NAME>
venue name iso-lang <ISO-LANG-CODE> <VENUE-NAME>
```

### Parameters

```
venue group [assembly|business|educational|industrial|institutional|mercantile|
outdoor|residential|storage|unspecified|utility-and-misc|vehicular] type
```

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| venue group      | Configures the venue group associated with this hotspot                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| assembly<br>type | Configures the venue group as assembly (1). This hotspot type is applicable to public assembly venues. <ul style="list-style-type: none"><li>• type – Specifies the venue type for this group. The options are:<ul style="list-style-type: none"><li>• &lt;0-255&gt; – Specifies an unlisted venue type number from 0 -255</li><li>• amphitheater – Specifies the venue type as amphitheater (4)</li><li>• amusement-park – Specifies the venue type as amusement park (5)</li><li>• arena – Specifies the venue type as arena (1)</li><li>• bar – Specifies the venue type as bar (12)</li><li>• coffee-shop – Specifies the venue type as a coffee shop (13)</li><li>• convention-centre – Specifies the venue type as a convention center (7)</li><li>• emergency-coordination-center – Specifies the venue type as a emergency coordination center (15)</li><li>• library – Specifies the venue type as a library (8)</li><li>• museum – Specifies the venue type as a museum (9)</li><li>• passenger-terminal – Specifies the venue type as a passenger terminal (3)</li><li>• place-of-worship – Specifies the venue type as a place of worship (6)</li><li>• restaurant – Specifies the venue type as a restaurant (10)</li><li>• stadium – Specifies the venue type as a stadium (2)</li><li>• theater – Specifies the venue type as a theater (11)</li><li>• unspecified – Specifies the venue type as not specified (0)</li><li>• zoo – Specifies the venue type as a zoo (14)</li></ul></li></ul> |

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| business type | <p>Configures the venue group as business (2). This hotspot type is applicable to business venues.</p> <ul style="list-style-type: none"> <li>• type – Specifies the venue type for this group. The options are: <ul style="list-style-type: none"> <li>• &lt;0-255&gt; – Specifies an unlisted venue type number from 0 -255</li> <li>• attorney – Specifies the venue type as the attorney’s office (9)</li> <li>• bank – Specifies the venue type as a bank (2)</li> <li>• doctor – Specifies the venue type as a doctor or dentist’s office (1)</li> <li>• fire-station – Specifies the venue type as a fire station (3)</li> <li>• police-station – Specifies the venue type as a police station (4)</li> <li>• post-office – Specifies the venue type as a post office (5)</li> <li>• professional-office – Specifies the venue type as a professional office (7)</li> <li>• research-and-development-facility – Specifies the venue type as a research facility (8)</li> <li>• unspecified – Specifies the venue type as not specified (0)</li> </ul> </li> </ul> |
| educational   | <p>Configures the venue group as educational (3). This hotspot type is applicable to educational institutions.</p> <ul style="list-style-type: none"> <li>• type – Specifies the venue type for this group. The options are: <ul style="list-style-type: none"> <li>• &lt;0-255&gt; – Specifies an unlisted venue type number from 0 -255</li> <li>• school-primary – Specifies the venue type as a primary school (1)</li> <li>• school-secondary – Specifies the venue type as a secondary school (2)</li> <li>• university – Specifies the venue type as a university or college (3)</li> <li>• unspecified – Specifies the venue type as not specified (0)</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                    |
| industrial    | <p>Configures the venue group as industrial (4). This hotspot type is applicable to industrial venues.</p> <ul style="list-style-type: none"> <li>• type – Specifies the venue type for this group. The options are: <ul style="list-style-type: none"> <li>• &lt;0-255&gt; – Specifies an unlisted venue type number from 0 -255</li> <li>• factory – Specifies the venue type as a factory (1)</li> <li>• unspecified – Specifies the venue type as not specified (0)</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| institutional | <p>Configures the venue group as institutional (4). This hotspot type is applicable to public health and other institutions.</p> <ul style="list-style-type: none"> <li>• type – Specifies the venue type for this group. The options are: <ul style="list-style-type: none"> <li>• &lt;0-255&gt; – Specifies an unlisted venue type number from 0 -255</li> <li>• group-home – Specifies the venue type as a group-home (4)</li> <li>• hospital – Specifies the venue type as a hospital (1)</li> <li>• long-term-care – Specifies the venue type as a long term care facility (2)</li> <li>• prison – Specifies the venue type as a prison or jail (5)</li> <li>• rehab – Specifies the venue type as a rehabilitation facility (3)</li> <li>• unspecified – Specifies the venue type as not specified (0)</li> </ul> </li> </ul>                                                                                                                                                                                                                                      |
| mercantile    | <p>Configures the venue group as mercantile (6). This hotspot type is applicable to public mercantile venues.</p> <ul style="list-style-type: none"> <li>• type – Specifies the venue type for this group. The options are: <ul style="list-style-type: none"> <li>• &lt;0-255&gt; – Specifies an unlisted venue type number from 0 -255</li> <li>• automotive – Specifies the venue type as a automotive service center (3)</li> <li>• gas-station – Specifies the venue type as a gas station (5)</li> <li>• grocery – Specifies the venue type as a grocery store (2)</li> <li>• mall – Specifies the venue type as a shopping mall (4)</li> <li>• retail – Specifies the venue type as a retail store (1)</li> <li>• unspecified – Specifies the venue type as not specified (0)</li> </ul> </li> </ul>                                                                                                                                                                                                                                                              |

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| outdoor     | <p>Configures the venue group as outdoor (11). This hotspot type is applicable to public outdoor venues.</p> <ul style="list-style-type: none"> <li>• type – Specifies the venue type for this group. The options are: <ul style="list-style-type: none"> <li>• &lt;0-255&gt; – Specifies an unlisted venue type number from 0 -255</li> <li>• bus-stop – Specifies the venue type as a bus stop (5)</li> <li>• city-park – Specifies the venue type as a city park (2)</li> <li>• kiosk – Specifies the venue type as a kiosk (6)</li> <li>• muni-mesh – Specifies the venue type as a muni-mesh (municipal wireless Wi-Fi) (1)</li> <li>• rest-area – Specifies the venue type as a rest area (3)</li> <li>• traffic-control – Specifies the venue type as a traffic control area (4)</li> <li>• unspecified – Specifies the venue type as not specified (0)</li> </ul> </li> </ul> |
| residential | <p>Configures the venue group as residential (7). This hotspot type is applicable to residential complexes.</p> <ul style="list-style-type: none"> <li>• type – Specifies the venue type for this group. The options are: <ul style="list-style-type: none"> <li>• &lt;0-255&gt; – Specifies an unlisted venue type number from 0 -255</li> <li>• boarding-house – Specifies the venue type as a boarding-house (4)</li> <li>• dorm – Specifies the venue type as a dormitory (3)</li> <li>• hotel – Specifies the venue type as a hotel or motel (2)</li> <li>• private – Specifies the venue type as a private residence (1)</li> <li>• unspecified – Specifies the venue type as not specified (0)</li> </ul> </li> </ul>                                                                                                                                                          |
| storage     | <p>Configures the venue group as storage (8). This hotspot type is applicable to storage groups.</p> <ul style="list-style-type: none"> <li>• type – Specifies the venue type for this group. The options are: <ul style="list-style-type: none"> <li>• &lt;0-255&gt; – Specifies an unlisted venue type number from 0 -255</li> <li>• unspecified – Specifies the venue type as not specified (0)</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| unspecified | <p>Configures the venue group as unspecified (0)</p> <ul style="list-style-type: none"> <li>• type – Specifies the venue type for this group. The options are: <ul style="list-style-type: none"> <li>• &lt;0-255&gt; – Specifies an unlisted venue type number from 0 -255</li> <li>• unspecified – Specifies the venue type as not specified (0)</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| utility-and-misc | <p>Configures the venue group as utility and miscellaneous (8)</p> <ul style="list-style-type: none"> <li>type – Specifies the venue type for this group. The options are: <ul style="list-style-type: none"> <li>&lt;0-255&gt; – Specifies an unlisted venue type number from 0 -255</li> <li>unspecified – Specifies the venue type as not specified (0)</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| vehicular        | <p>Configures the venue group as vehicular (7). This hotspot type is applicable to mobile venues.</p> <ul style="list-style-type: none"> <li>type – Specifies the venue type for this group. The options are: <ul style="list-style-type: none"> <li>&lt;0-255&gt; – Specifies an unlisted venue type number from 0 -255</li> <li>airplane – Specifies the venue type as an airplane (2)</li> <li>auto – Specifies the venue type as an automobile or truck (1)</li> <li>bus – Specifies the venue type as a bus (3)</li> <li>ferry – Specifies the venue type as a ferry (5)</li> <li>motor-bike – Specifies the venue type as a motor bike (7)</li> <li>ship – Specifies the venue type as a ship or boat (5)</li> <li>train – Specifies the venue type as a train (6)</li> <li>unspecified – Specifies the venue type as not specified (0)</li> </ul> </li> </ul> |

operator name <VENUE-NAME>

|             |                                                                                                                                                      |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| name <WORD> | <p>Configures the venue name in English</p> <ul style="list-style-type: none"> <li>&lt;WORD&gt; – Specify the venue name in ASCII format.</li> </ul> |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------|

operator name iso-lang <ISO-LANG-CODE> <VENUE-NAME>

|                                            |                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| name iso-lang <ISO-LANG-CODE> <VENUE-NAME> | <p>Configures a non-English venue name</p> <ul style="list-style-type: none"> <li>iso-lang &lt;ISO-LANG-CODE&gt; – Identifies the language by its ISO 639 language code (for example, 'chi-chinese' or 'spa-spanish').</li> <li>&lt;ISO-LANG-CODE&gt; – Specify the 3 character iso-639 language code.</li> <li>&lt;VENUE-NAME&gt; – Specify the venue name as a hexadecimal code,</li> </ul> |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```

nx9500-6C8809(config-passpoint-policy-test)#venue name testShop
nx9500-6C8809(config-passpoint-policy-test)#venue group assembly type coffee-shop
nx9500-6C8809(config-passpoint-policy-test)#show context
passpoint-policy test
 access-network-type chargeable-public
 connection-capability ip-protocol 2 port 10 closed
 nai-realm example
 eap-method 1 ttls auth-param vendor hex 00001E
 eap-method 2 rsa-public-key auth-param credential cert
 net-auth-type accept-terms url www.test.com
 operator name exampleoperator
 roam-consortium hex 223344
 venue group assembly type coffee-shop
 venue name testShop
 3gpp mcc 505 mnc 14
 osu ssid test
 osu provider test
 name testOSU
 method soap-xml-spp priority 2
 nai test.org
 server-url test.exampe.com
nx9500-6C8809(config-passpoint-policy-test)#

```

## Related Commands

|                                                                                        |
|----------------------------------------------------------------------------------------|
| <code>no</code> Removes the venue group and type configured with this passpoint policy |
|----------------------------------------------------------------------------------------|

### wan-metrics

Configures the WAN performance metrics for this hotspot. This command configures the upstream and downstream speeds associated with this hotspot. The upstream and downstream speed values (in Kbps) are estimates of the bandwidth available on the WAN. This information is returned in response to client ANQP query, and is useful for clients having a minimum and/or large bandwidth requirement.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
wan-metrics down-speed <0-4294967295> up-speed <0-4294967295>
```

#### Parameters

```
wan-metrics down-speed <0-4294967295> up-speed <0-4294967295>
```

|                           |                                                                                                                                                             |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wan-metrics               | Specifies the WAN metrics for the up and down traffic                                                                                                       |
| down-speed <0-4294967295> | Configures the down stream traffic speed <ul style="list-style-type: none"><li>• &lt;0-4294967295&gt; - Specify a value from 0 - 4294967295 Kbps.</li></ul> |
| up-speed <0-4294967295>   | Configures the up stream traffic speed <ul style="list-style-type: none"><li>• &lt;0-4294967295&gt; - Specify a value from 0 - 4294967295 Kbps.</li></ul>   |

#### Examples

```
nx9500-6C8809(config-passpoint-policy-test)#wan-metrics down-speed 2000 up-speed 2000
nx9500-6C8809(config-passpoint-policy-test)#show context
passpoint-policy test
 access-network-type chargeable-public
 connection-capability ip-protocol 2 port 10 closed
 nai-realm example
 eap-method 1 ttls auth-param vendor hex 00001E
 eap-method 2 rsa-public-key auth-param credential cert
 net-auth-type accept-terms url www.test.com
 operator name exampleoperator
 roam-consortium hex 223344
 venue group assembly type coffee-shop
 venue name testShop
 wan-metrics down-speed 2000 up-speed 2000
 3gpp mcc 505 mnc 14
 osu ssid test
 osu provider test
 name testOSU
 method soap-xml-spp priority 2
 nai test.org
 server-url test.exampe.com
nx9500-6C8809(config-passpoint-policy-test)#
```



## Related Commands

|                                                                                |
|--------------------------------------------------------------------------------|
| <code>no</code> Removes the WAN metrics configuration on this passpoint policy |
|--------------------------------------------------------------------------------|

`no`

Removes or reverts the passpoint policy settings

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
no [3gpp|access-network-type|connection-capability|domain-name|hessid|internet|
ip-address-type|nai-realm|net-auth-type|operator|osu|roam-consortium|venue|wan-metrics]
```

### Parameters

```
no <PARAMETERS>
```

|                                    |                                                  |
|------------------------------------|--------------------------------------------------|
| <code>no &lt;PARAMETERS&gt;</code> | Removes or reverts the passpoint policy settings |
|------------------------------------|--------------------------------------------------|

### Examples

The following example shows the passpoint policy 'test' settings before the 'no' commands are executed:

```
nx9500-6C8809(config-passpoint-policy-test)#show context
passpoint-policy test
 access-network-type chargeable-public
 connection-capability ip-protocol 2 port 10 closed
 nai-realm example
 eap-method 1 ttls auth-param vendor hex 00001E
 eap-method 2 rsa-public-key auth-param credential cert
 net-auth-type accept-terms url www.test.com
 operator name exampleoperator
 roam-consortium hex 223344
 venue group assembly type coffee-shop
 venue name testShop
 wan-metrics down-speed 2000 up-speed 2000
 3gpp mcc 505 mnc 14
 osu ssid test
 osu provider test
 name testOSU
 method soap-xml-spp priority 2
 nai test.org
 server-url test.exampe.com
nx9500-6C8809(config-passpoint-policy-test)#
nx9500-6C8809(config-passpoint-policy-test)#no access-network-type
nx9500-6C8809(config-passpoint-policy-test)#no nai-realm example
nx9500-6C8809(config-passpoint-policy-test)#no 3gpp mcc 505 mnc 14
nx9500-6C8809(config-passpoint-policy-test)#no internet
nx9500-6C8809(config-passpoint-policy-test)#show context
passpoint-policy test
 connection-capability ip-protocol 2 port 10 closed
 no internet
 net-auth-type accept-terms url www.test.com
```

---

```
operator name exampleoperator
roam-consortium hex 223344
venue group assembly type coffee-shop
venue name testShop
wan-metrics down-speed 2000 up-speed 2000
osu ssid test
osu provider test
 name testOSU
 method soap-xml-spp priority 2
 nai test.org
 server-url test.exampe.com
nx9500-6C8809(config-passpoint-policy-test)#
```

# CRYPTO CMP POLICY

## CRYPTO-CMP-POLICY

---

This chapter summarizes the crypto CMP (certificate management protocol) policy commands in the CLI command structure.

CMP is an Internet protocol designed to enable devices (access point, wireless controller, or service platform) to obtain and manage digital certificates in a PKI (Public Key Infrastructure) network. A CA (Certificate Authority) issues the certificates using the defined CMP.

WiNG CMP implementation allows you to configure a crypto CMP policy that enables auto installation and auto management of device certificates. When configured and implemented on a device, the crypto CMP policy allows the device to automatically trigger a certification request to a configured, CMP supported CA server. Once the certificate is validated and confirmed from the CA server it is saved on the device and becomes part of the trustpoint. During the creation of the CMP policy the trustpoint is assigned a name and client information. You can use a manually created trustpoint for one service (like HTTPS) and use the CMP generated trustpoint for RADIUS EAP certificate based authentication.

Use the (config) instance to configure a crypto CMP policy. To navigate to the crypto CMP policy configuration instance, use the following commands:

```
<DEVICE>(config)#crypto-cmp-policy <CRYPTO-CMP-POLICY-NAME>
nx9500-6C8809(config)#crypto-cmp-policy CMPPolicy
nx9500-6C8809(config-cmp-policy-CMPPolicy)#?
CMP Policy Mode commands:
 ca-server CMP CA Server configuration commands
 cert-key-size Set key size for certificate request
 cert-renewal-timeout Trigger a cert renewal request on timeout
 cross-cert-validate Validate cross-cert using factory-cert
 hash-algorithm Set hash algorithm for certificate request
 no Negate a command or set its defaults
 subjectAltName Configure subjectAltName value
 trustpoint Trustpoint for CMP
 use Set setting to use

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal
nx9500-6C8809(config-cmp-policy-CMPPolicy)#
```

This chapter is organized as follows:

- [crypto-cmp-policy-instance](#)
- [other-cmp-related-commands](#)

## crypto-cmp-policy-instance

The following table summarizes crypto CMP policy configuration commands:

**Table 67: Crypto-CMP-Policy Config Mode Commands**

| Description                                    | Command                                                                                                                                                                             |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>ca-server</code>                         | Configures the CA server details                                                                                                                                                    |
| <code>cert-key-size</code> on page 1833        | Configures the size of the key associated with a certificate request                                                                                                                |
| <code>cert-renewal-timeout</code> on page 1834 | Configures a certificate renewal timeout in days                                                                                                                                    |
| <code>cross-cert-validate</code> on page 1835  | Enables validation of the cross certificate with the factory certificate                                                                                                            |
| <code>hash-algorithm</code> on page 1836       | Configures the hashing algorithm to be used by the CA to sign the digital certificate. This information is sent in the request for certification (new or renewal) to the CA server. |
| <code>subjectAltName</code> on page 1836       | Configures an alternate subject name for this CMP policy                                                                                                                            |
| <code>trustpoint</code>                        | Configures a trustpoint and its associated information, such as the subject name, the sender's (device requesting certification) details, and the recipient's (CA) details          |
| <code>use</code>                               | Associates a device's autogen-uniqueid with this crypto CMP policy                                                                                                                  |
| <code>no</code>                                | Removes the crypto CMP policy settings                                                                                                                                              |



### Note

The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore ( \_ ) character. In other words, the name of a device cannot contain an underscore.



### Note

For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see [COMMON COMMANDS](#).

### *ca-server*

Configures the primary and secondary CMP CA server details.

The CA is an external network authority (usually a trusted third-party server) that generates and issues digital certificates in response to requests received from network devices. Use this command to configure the primary and secondary CA server details, such as name of the device hosting the CA server, the port used to access the CA server, and the path where the certificate is stored. Once defined, devices using this CMP policy automatically send requests to the specified primary CA server, and retrieve the certificate from the specified location. If the primary CA server is not reachable, the requests are sent to the secondary CA server.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000

- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
ca-server [primary|secondary] host <IP> port <1-65535> path <PATH>
```

### Parameters

```
ca-server [primary|secondary] host <IP> port <1-65535> path <PATH>
```

|                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ca-server<br>[primary <br>secondary] | <p>Configures the primary and secondary CMP CA server details (IPv4 address, port, and path)</p> <ul style="list-style-type: none"> <li>• primary – Configures the primary CMP CA server’s details</li> <li>• secondary – Configures the secondary CMP CA server’s details</li> </ul> <p>The secondary CMP CA is used in case the primary CA server is not reachable. CA server settings are required to complete CMP requests.</p> |
| host <IP>                            | <p>Configures IP address or hostname of the device hosting the CA server</p> <ul style="list-style-type: none"> <li>• &lt;IP/HOSTNAME&gt; – Specify the IP address or hostname.</li> </ul>                                                                                                                                                                                                                                          |
| port <PORT-<br>NUMBER>               | <p>Configures IPv4 address of the device hosting the primary/secondary CA server</p> <ul style="list-style-type: none"> <li>• &lt;IP/HOSTNAME&gt; – Specify the server’s IPv4 address.</li> </ul>                                                                                                                                                                                                                                   |
| port <1-65535>                       | <p>Configures the port on which the primary/secondary CA server can be reached</p> <ul style="list-style-type: none"> <li>• &lt;1-65535&gt; – Specify the port number from 1 - 65535.</li> </ul>                                                                                                                                                                                                                                    |
| path <PATH>                          | <p>Configures the path or filename of the primary/secondary CMP CA certificate. Enter the complete relative path to the file on the server.</p> <ul style="list-style-type: none"> <li>• &lt;PATH&gt; – Specify the path. Once specified, the certificate is downloaded from this location and installed on the device.</li> </ul>                                                                                                  |

### Examples

```
ap6522-D8273A(config-cmp-policy-CMP)#ca-server primary host 192.168.8.74 port 8 path cmp
ap6522-D8273A(config-cmp-policy-CMP)#show context
crypto-cmp-policy CMP
ca-server primary host 192.168.8.74 port 80 path cmp
ap6522-D8273A(config-cmp-policy-CMP)#
```

### Related Commands

|    |                                                            |
|----|------------------------------------------------------------|
| no | Removes the configured primary/secondary CA server details |
|----|------------------------------------------------------------|

### cert-key-size

Configures the size of the key associated with a certificate request

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
cert-key-size [2048|3072|4096]
```

## Parameters

`cert-key-size [2048|3072|4096]`

|                                             |                                                                                                                                                                                                                                                                                     |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>cert-key-size [2048 3072 4096]</code> | Configures the certificate request key size. The options are: <ul style="list-style-type: none"><li>• 2048 – Sets the key size to 2048 bits. This is the default setting.</li><li>• 3072 – Sets the key size to 3072 bits</li><li>• 4096 – Sets the key size to 4096 bits</li></ul> |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-cmp-policy-test)#cert-key-size 3072
nx9500-6C8809(config-cmp-policy-test)#show context
crypto-cmp-policy test
 cert-key-size 3072
 ca-server primary host 192.168.8.74 port 8 path cmp
nx9500-6C8809(config-cmp-policy-test)#
```

## Related Commands

|                              |                                                                 |
|------------------------------|-----------------------------------------------------------------|
| <code>no</code> on page 1839 | Reverts the certificate request key size to default (2048 bits) |
|------------------------------|-----------------------------------------------------------------|

### *cert-renewal-timeout*

Configures a certificate renewal timeout in days. This is the number of days, before the expiration of the device's certificate, that a certificate renewal is triggered.

The expiration of device's certificate is checked once a day. When a certificate is about to expire a certificate renewal is initiated with the dedicated CMP CA server resource through an existing IPSec tunnel. If the tunnel is not established, the CMP renewal request is not sent. If a renewal succeeds the newly obtained certificate overwrites an existing certificate. If the renewal fails, an error is logged.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

`cert-renewal-timeout <1-60>`

## Parameters

`cert-renewal-timeout <1-60>`

|                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>cert-renewal-timeout &lt;1-60&gt;</code> | Configures the certificate renewal timeout in days. This is the number of days, before the expiration of the device's certificate, that a certificate renewal is triggered. Once the configured time is completed, the device triggers a certificate renewal request. <ul style="list-style-type: none"><li>• &lt;1-60&gt; – Specify a value from 1 - 60 days. The default is fourteen (14) days. Therefore, by default a device triggers certificate renewal request 14 days before its certificate expires.</li></ul> |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
ap6522-D8273A(config-cmp-policy-CMP)#cert-renewal-timeout 60
ap6522-D8273A(config-cmp-policy-CMP)#show context
crypto-cmp-policy CMP
 cert-renewal-timeout 60
 ca-server primary host 192.168.8.74 port 8 path cmp
ap6522-D8273A(config-cmp-policy-CMP)#
```

## Related Commands

|                                 |                                                              |
|---------------------------------|--------------------------------------------------------------|
| <a href="#">no</a> on page 1839 | Reverts the certificate renewal timeout to default (14 days) |
|---------------------------------|--------------------------------------------------------------|

### *cross-cert-validate*

Enables validation of the cross certificate using the factory certificate. When enabled, the obtained cross-certificate is validated against the operator's certificate configured on the device. An error message is displayed in case the cross-certificate is not obtained or if the cross-certificate is found to be invalid. This option is disabled by default.



#### Note

To configure the operator certificate, in the device configuration mode execute the **trustpoint > cmp-auth-operator** command. For more information, see [trustpoint \(device-config-mode\)](#) on page 1282.

## Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
cross-cert-validate
```

## Parameters

None

## Examples

```
nx9500-6C8809(config-cmp-policy-test)#cross-cert-validate
nx9500-6C8809(config-cmp-policy-test)#show context
crypto-cmp-policy test
 cert-key-size 3072
 cross-cert-validate
 ca-server primary host 192.168.8.74 port 8 path cmp
nx9500-6C8809(config-cmp-policy-test)#
```

## Related Commands

|                                 |                                                                           |
|---------------------------------|---------------------------------------------------------------------------|
| <a href="#">no</a> on page 1839 | Disables validation of the cross certificate with the factory certificate |
|---------------------------------|---------------------------------------------------------------------------|

## hash-algorithm

Configures the hashing algorithm to be used to sign the digital certificate. This information is sent to the CA in the request for certification (new or renewal). The CA uses the hash algorithm specified here to sign the digital certificate.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
hash-algorithm [sha1|sha256|sha384|sha512]
```

### Parameters

```
hash-algorithm [sha1|sha256|sha384|sha512]
```

|                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| hash-algorithm [sha1 sha256 sha384 sha512] | <p>Configures the hashing algorithm type. The options are:</p> <ul style="list-style-type: none"><li>• sha1 - Uses SHA1 (Secure Hash Algorithm 1) hash function. This is the default setting.</li><li>• sha256 - Uses SHA256 hash function.</li><li>• sha384 - Uses SHA384 hash function.</li><li>• sha512 - Uses SHA512 hash function.</li></ul> <p><b>Note:</b> The <b>sha256</b>, <b>sha384</b> and <b>sha512</b> hash functions belong to the SHA-2 family of algorithms.</p> |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config-cmp-policy-CMPPolicy)#hash-algorithm sha512
nx9500-6C8809(config-cmp-policy-CMPPolicy)#show context
crypto-cmp-policy CMPPolicy
 hash-algorithm sha512
nx9500-6C8809(config-cmp-policy-CMPPolicy)#
```

### Related Commands

|                 |                                                         |
|-----------------|---------------------------------------------------------|
| no on page 1839 | Reverts the Hash Algorithm used to default value (sha1) |
|-----------------|---------------------------------------------------------|

## subjectAltName

Configures the subjectAltName identity for this CMP policy

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000



## Syntax

```
subjectAltName [address <IP>|dn <DISTINGUISHED-NAME>|email <EMAIL-ID>|fqdn <FQDN>|
string <USER-DEFINED-STRING>]
```

## Parameters

```
subjectAltName [address <IP>|dn <DISTINGUISHED-NAME>|email <EMAIL-ID>|fqdn <FQDN>|
string <USER-DEFINED-STRING>]
```

```
subjectAltName [address <IP>|dn
<DISTINGUISHED-NAME>|email
<EMAIL-ID>|fqdn <FQDN>|string
<USER-DEFINED-STRING>]
```

Configures an alternative name (disguise) for the subject using one of the following options:

- address <IP> – Uses IP address as identity
  - <IP> – Specify the IP address.
- dn <DISTINGUISHED-NAME> – Uses distinguished name as identity
  - <DISTINGUISHED-NAME> – Specify the DISTINGUISHED-NAME.
- email <EMAIL-ID> – Uses e-mail address as identity
  - <EMAIL-ID> – Specify the e-mail address.
- fqdn <FQDN> – Uses FQDN as identity
  - <FQDN> – Specify the FQDN.
- string <USER-DEFINED-STRING> – Uses a user specified name as identity
  - <USER-DEFINED-STRING> – Specify the string to use as identity.

**Note:** The alternative name value should not exceed 128 characters.

## Examples

```
ap6522-D8273A(config-cmp-policy-CMP)#subjectAltName dn TechPubsCA
ap6522-D8273A(config-cmp-policy-CMP)#show context
crypto-cmp-policy CMP
 cert-update
 cert-renewal-timeout 60
 ca-server primary host 192.168.8.74 port 8 path cmp
 subjectAltName dn TechPubsCA
ap6522-D8273A(config-cmp-policy-CMP)#
```

## Related Commands

|                              |                                                                     |
|------------------------------|---------------------------------------------------------------------|
| <code>no</code> on page 1839 | Removes the subjectAltName identity configured with this CMP policy |
|------------------------------|---------------------------------------------------------------------|

### *trustpoint*

Configures a trustpoint and its associated information, such as the subject name, the sender's (device requesting certification) details, and the recipient's (CA) details. This information is needed to obtain the certificate from the CA server using CMP.

Each certificate is digitally signed by a CA and contains device-specific information, such as device name, IP address, serial number. It helps to uniquely identify a device.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000

- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
trustpoint <TRUSTPOINT-NAME> subject-name <WORD> secret [0 <WORD>|2 <WORD>]
reference-id <WORD> sender-name <WORD> [recipient-name <WORD>|ca-psk <CERT-PATH>]
```

## Parameters

```
trustpoint <TRUSTPOINT-NAME> subject-name <WORD> secret [0 <WORD>|2 <WORD>]
reference-id <WORD> sender-name <WORD> [recipient-name <WORD>|ca-psk <CERT-PATH>]
```

|                                 |                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| trustpoint<br><TRUSTPOINT-NAME> | Configures a trustpoint name (should not exceed 32 characters) <ul style="list-style-type: none"> <li>• &lt;TRUSTPOINT-NAME&gt; - Specify the trustpoint's name.</li> </ul>                                                                                                                                                                                               |
| subject-name <WORD>             | Configures a subject name for this trustpoint. The subject name should uniquely identify the certificate and should not exceed 512 characters in length.                                                                                                                                                                                                                  |
| secret [0 <WORD> 2 <WORD>]      | Configures the secret used to encrypt the trustpoint. The secret should not exceed 128 characters in length. <ul style="list-style-type: none"> <li>• 0 &lt;WORD&gt; - Configures a clear text password</li> <li>• 2 &lt;WORD&gt; - Configures an encrypted password <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specify the password.</li> </ul> </li> </ul> |
| reference-id <WORD>             | Configures the reference ID. The CA server uses this information to identify the shared secret key used. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specify the reference ID.</li> </ul>                                                                                                                                                                     |
| sender-name <WORD>              | Configures the sender's name. The CA server uses this information to identify the shared secret key used. The sender's name should not exceed 512 characters in length. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specify the sender name.</li> </ul>                                                                                                       |
| recipient-name                  | Configures the recipient's name. The CA server uses this information to validate the request. The recipient's name should not exceed 256 characters in length.                                                                                                                                                                                                            |
| ca-psk <CERT-PATH>              | Configures the certificate path for the server certificate <ul style="list-style-type: none"> <li>• &lt;CERT-PATH&gt; - Specify the certificate path.</li> </ul>                                                                                                                                                                                                          |

## Examples

```
ap6522-D8273A(config-cmp-policy-CMP)#trustpoint cmp-test subject-name "CN=ExampleCompany, O=Example Company" secret 0 test-secret reference-id 123456 sender-name "CN=ExampleCompany.com, O=Example Company" recipient-name "O=Example Company, CN=ExampleCompany.com"
ap6522-D8273A(config-cmp-policy-CMP)#
ap6522-D8273A(config-cmp-policy-CMP)#show context
crypto-cmp-policy CMP
cert-update
cert-renewal-timeout 60
ca-server primary host 192.168.8.74 port 8 path cmp
trustpoint cmp-test subject-name "CN=ExampleCompany, O=Example Company" secret 0 test-secret reference-id 123456 sender-name "CN=ExampleCompany.com, O=Example Company" recipient-name "O=Example Company, CN=ExampleCompany.com"
subjectAltName dn TechPubsCA
ap6522-D8273A(config-cmp-policy-CMP)#
```

## Related Commands

|           |                                                               |
|-----------|---------------------------------------------------------------|
| <b>no</b> | Removes the trustpoint associated with this crypto CMP policy |
|-----------|---------------------------------------------------------------|

*use*

Associates a device's autogen-uniqueid with this crypto CMP policy

A device's autogen-uniqueid is a combination of a user-defined string (prefix or suffix) and a substitution token. The WiNG software implementation provides two built-in substitution tokens: \$SN and \$MiNT-ID that represent the device's serial number and MiNT ID respectively. These substitution tokens are internally retrieved and combined with the user-defined string to auto generate a unique identity for a device.

To auto generate the device's unique ID, in the device configuration mode execute the following command:

```
autogen-uniqueid <WORD>
```

For more information on the autogen-uniqueid command, see [autogen-uniqueid](#) on page 883.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
use autogen-uniqueid
```

### Parameters

```
use autogen-uniqueid
```

`use autogen-uniqueid` Associates a device's autogen-uniqueid with this crypto CMP policy. The device's autogen-uniqueid should be existing and configured.

### Examples

```
ap6522-D8273A(config-cmp-policy-CMP)#use autogen-uniqueid
ap6522-D8273A(config-cmp-policy-CMP)#show context
crypto-cmp-policy CMP
 cert-update
 cert-renewal-timeout 60
 use autogen-uniqueid
 ca-server primary host 192.168.8.74 port 8 path cmp
 trustpoint cmp-test subject-name "CN=ExampleCompany, O=Example Company" secret 0 test-
 secret reference-id 123456 sender-name "CN=ExampleCompany.com, O=Example Company"
 recipient-name "O=Example Company, CN=ExampleCompany.com"
 subjectAltName dn TechPubsCA
ap6522-D8273A(config-cmp-policy-CMP)#
```

### Related Commands

`no` Removes the device's autogen-uniqueid associated with this crypto CMP policy

*no*

Removes or reverts this crypto CMP policy settings

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
no [ca-server <SERVER-NAME>|cert-key-size|cert-renewal-timeout|cross-cert-validate|
hash-algorithm|subjectAltName|trustpoint <TRUSTPOINT-NAME>|use autogen-uniqueid]
```

### Parameters

```
no <PARAMETERS>
```

|                 |                                                    |
|-----------------|----------------------------------------------------|
| no <PARAMETERS> | Removes or reverts this crypto CMP policy settings |
|-----------------|----------------------------------------------------|

### Examples

```
ap6522-D8273A(config-cmp-policy-CMP)#show context
cert-update
cert-renewal-timeout 60
use autogen-uniqueid
ca-server primary host 192.168.8.74 port 8 path cmp
trustpoint cmp-test subject-name "CN=ExampleCompany, O=Example Company" secret 0 test-
secret reference-id 123456 sender-name "CN=ExampleCompany.com, O=Example Company"
recipient-name "O=Example Company, CN=ExampleCompany.com"
subjectAltName dn TechPubsCA
ap6522-D8273A(config-cmp-policy-CMP)#
ap6522-D8273A(config-cmp-policy-CMP)#no cert-renewal-timeout
ap6522-D8273A(config-cmp-policy-CMP)#no subjectAltName
ap6522-D8273A(config-cmp-policy-CMP)#show context
cert-update
use autogen-uniqueid
ca-server primary host 192.168.8.74 port 8 path cmp
trustpoint cmp-test subject-name "CN=ExampleCompany, O=Example Company" secret 0 test-
secret reference-id 123456 sender-name "CN=ExampleCompany.com, O=Example Company"
recipient-name "O=Example Company, CN=ExampleCompany.com"
ap6522-D8273A(config-cmp-policy-CMP)#
```

## other-cmp-related-commands

The following table summarizes other commands associated with the implementation of the crypto CMP policy:

**Table 68: Other-CMP-Related Commands**

| Command           | Description                                                                                                                       |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <code>use</code>  | Associates a crypto CMP policy with a device                                                                                      |
| <code>show</code> | Displays current status of CMP requests in progress. This command also displays trustpoint details (CMP and non-CMP trustpoints). |

## use (other-cmp-related-commands)

Applies a crypto CMP policy to a device. Once CMP enabled, the device automatically requests for a certificate from the CA server and installs it. After applying the CMP policy, commit and write the change to memory. This is needed to apply this configuration across reboots.

To apply a CMP policy on a device, navigate to the device's config-device mode and execute the **use > crypto-cmp-policy <CRYPTO-CMP-POLICY-NAME>** command.

*Supported in the following platforms:*

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
use crypto-cmp-policy <CRYPTO-CMP-POLICY-NAME>
```

### Parameters

```
use crypto-cmp-policy <CRYPTO-CMP-POLICY-NAME>
```

|                                        |                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cmp-policy<br><CRYPTO-CMP-POLICY-NAME> | Applies an existing crypto CMP policy on this device. When associated with a profile, the crypto CMP policy is applied to all devices using the profile. <ul style="list-style-type: none"><li>• &lt;CRYPTO-CMP-POLICY-NAME&gt; - Specify the crypto CMP policy name. Should be existing and configured.</li></ul> |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
ap6522-D8273A(config-device-00-11-3F-D8-27-3A)#use crypto-cmp-policy CMP
ap6522-D8273A(config-device-00-11-3F-D8-27-3A)#commit
```

## show (other-cmp-related-commands)

Displays current status of CMP requests in progress. This command also displays trustpoint details (CMP and non-CMP trustpoints).

*Supported in the following platforms:*

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
show crypto [cmp|pki]
show crypto cmp request status {on <DEVICE-NAME>}
show crypto pki trustpoints {<TRUSTPOINT-NAME>|all} {on <DEVICE-NAME>}
```

### Parameters

```
show crypto cmp request status {on <DEVICE-NAME>}
```

|                                            |                                                                                                                                                                                                                                                                                        |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show crypto cmp request {on <DEVICE-NAME>} | <p>Displays the current status of all on-going CMP requests</p> <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; - Optional. Optionally specify the name of the AP, wireless controller, or service platform to view CMP request status on a specified device.</li> </ul> |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
show crypto pki trustpoints {<TRUSTPOINT-NAME>|all} {on <DEVICE-NAME>}
```

|                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show pki trustpoints {<TRUSTPOINT-NAME> all} on <DEVICE-NAME> | <p>Displays all trustpoints including CMP generated trustpoints</p> <ul style="list-style-type: none"> <li>&lt;TRUSTPOINT-NAME&gt; - Optional. Specify a trustpoint name. Displays details of the trustpoint identified by the &lt;TRUSTPOINT-NAME&gt; parameter.</li> <li>all - Optional. Displays details of all configured trustpoints <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; - Optional. Specify the name of the AP, wireless controller, or service platform to view trustpoints configured on a specified device.</li> </ul> </li> </ul> |
|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
ap6522-D8273A#show crypto pki trustpoints
```

```

TRUSTPOINT KEY NAME VALID UNTIL

cmp-test cmp-test-key Fri May 9 09:44:22
2014 GMT
default-trustpoint default_rsa_key Fri Dec 30 00:00:40
2022 GMT

```

```
ap6522-D8273A#
ap6522-D8273A(config)#show crypto cmp request status
CMP Request Status: cmp-complete
```

```
ap6522-D8273A#
```

# ROAMING ASSIST POLICY

## ROAMING ASSIST POLICY

---

This chapter summarizes the Roaming Assist Policy commands in the CLI command structure.

By constantly monitoring a client's packets and the RSSI (received signal strength indicator) of a given client by a group of access points, decision can be made on the optimal access point to which the client needs to roam. Then forcefully direct the client to the optimal access point.

The threshold intervals are configurable and can be adjusted based on the client load.

Use the (config) instance to configure a roaming assist policy. To navigate to the roaming assist policy configuration instance, use the following commands:

```
<DEVICE> (config) roaming-assist-policy <ROAMING-ASSIST-POLICY-NAME>
nx9500-6C8809(config)roaming-assist-policy test
nx9500-6C8809(config-roaming-assist-policy-test)#?
Roaming Assist Mode commands:
 action Configure action - action is deauth / log /
 assisted-roam
 aggressiveness Configure the roaming aggressiveness for a wireless
 client
 detection-threshold Configure the detection threshold - when exceeded,
 client monitoring starts
 disassoc-time Configure the disassociation time - time after which a
 disassociation is sent
 handoff-count Configure the handoff count - number of times client
 can exceed handoff threshold
 handoff-threshold Configure the handoff threshold - when exceeds an
 action is taken.
 monitoring-interval Configure the monitoring interval - interval at which
 client monitoring occurs
 no Negate a command or set its defaults
 sampling-interval Configure the sampling interval - interval at which
 client rssi values are checked

 clrscr Clears the display screen
 commit Commit all changes made in this session
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

nx9500-6C8809(config-roaming-assist-policy-test)#
```

### roaming-assist-policy commands

The following table summarizes the roaming-assist-policy configuration mode commands:

Table: Roaming Assist Policy Config Mode Commands

| Command                                          | Description                                                                           |
|--------------------------------------------------|---------------------------------------------------------------------------------------|
| <a href="#">action</a> on page 1844              | Specifies the action to be invoked on the client                                      |
| <a href="#">aggressiveness</a> on page 1845      | Configures a roaming aggressiveness value for wireless clients                        |
| <a href="#">detection-threshold</a> on page 1846 | Configure detection-threshold interval value                                          |
| <a href="#">disassoc-time</a> on page 1847       | Configures the disassociation interval                                                |
| <a href="#">handoff-count</a> on page 1847       | Configures the handoff-count value                                                    |
| <a href="#">handoff-threshold</a> on page 1848   | Configures the handoff-threshold value                                                |
| <a href="#">monitoring-interval</a> on page 1849 | Configures the client monitoring interval                                             |
| <a href="#">sampling interval</a> on page 1850   | Configures the interval at which clients are sampled to determine their RSSI value    |
| <a href="#">no</a> on page 1850                  | Removes or reverts this roaming assist policy settings based on the parameters passed |



#### Note

For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see [COMMON COMMANDS](#).



#### Note

The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore ( \_ ) character. In other words, the name of a device cannot contain an underscore.

### *action*

Specifies the action invoked on the client once it reaches a specified threshold value. The threshold values are configured based on the client load.

#### **Supported in the following platforms:**

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### **Syntax**

```
action [assisted-roam|deauth|log]
```

#### **Parameters**

```
action [assisted-roam|deauth|log]
```



|                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| action<br>[assisted-roam <br>deauth log] | <p>Configures the action invoked on the client once it reaches the specified threshold value. The options are:</p> <ul style="list-style-type: none"> <li>assisted-roam – Provides 802.11v assisted roaming facility to the client</li> <li>deauth – De-authenticates the client. This is the default setting.</li> <li>log – Generates a log</li> </ul> <p><b>Note:</b> In all three cases an event is generated. However, the message generated differs and is based on the action specified.</p> |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```

nx9500-6C8809(config-roaming-assist-policy-test)#action log
nx9500-6C8809(config-roaming-assist-policy-test)#show context
roaming-assist-policy test
 action log
nx9500-6C8809(config-roaming-assist-policy-test)#

```

### Related Commands

|                 |                                       |
|-----------------|---------------------------------------|
| no on page 1850 | Removes the configured action details |
|-----------------|---------------------------------------|

### *aggressiveness*

Configures a roaming aggressiveness value for wireless clients. Configuring this value increases the client's roaming capabilities in scenarios where the client's location is likely to change drastically and suddenly. For example, when a client hops on to a train that speeds up quickly. In such a scenario, the access point receives a maximum of 2 (two) messages, from the client, having relatively low RSSI value. This results in a decaying-average, which is above the specified handover-threshold value. Consequently, the client is unable to roam.

#### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
aggressiveness [highest|lowest|medium|medium-high|medium-low]
```

#### Parameters

```
aggressiveness [highest|lowest|medium|medium-high|medium-low]
```

aggressiveness [highest|lowest|medium|medium-high|medium-low]

Configures a roaming aggressiveness value for wireless clients. The options are:

- highest – De-authenticates client in case of any degradation in the client's link quality. When selected, the access point considers only the RSSI value of the last message received from the client.
- lowest – De-authenticates client only in case of significant degradation in the client's link quality. When selected, the access point uses a weighted average [80% of decaying average + 20% of last seen RSSI] as the final reported RSSI value. This is the default setting.
- medium – This is an intermediate setting between not roaming and performance.
- medium-high – Allows roaming even if performance goes down. When selected, the access point calculates the client's signal strength based on average received signal as well as last received signal level, weighted towards the last received value.
- medium-low – Allows roaming even if performance goes average. When selected, the access point calculates the client's signal strength based on average received signal as well as last received signal level, weighted towards the average value.

### Examples

```
nx9500-6C8809(config-roaming-assist-policy-test)#aggressiveness medium-high
nx9500-6C8809(config-roaming-assist-policy-test)#show context
roaming-assist-policy test
 aggressiveness medium-high
 action log
nx9500-6C8809(config-roaming-assist-policy-test)#
```

### Related Commands

`no` on page 1850

Reverts the aggressiveness value to default (lowest)

### *detection-threshold*

Specifies the detection-threshold determining when a client is monitored

#### Supported in the following platforms:

- Access Points – AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers – RFS 4000
- Service Platforms – NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

#### Syntax

```
detection-threshold <-100--40>
```

#### Parameters

```
detection-threshold <-100--40>
```

detection-threshold  
<-100--40>

Configures the detection threshold value determining when a client is monitored. The clients with bad RSSI values are monitored more frequently.

- <-100--40> – Specify the RSSI value from -100 dBm - -40 dBm. The default is -75 dBm.

## Examples

```
nx9500-6C8809(config-roaming-assist-policy-test)#detection-threshold -90
nx9500-6C8809(config-roaming-assist-policy-test)#show context
roaming-assist-policy test
 aggressiveness medium-high
 detection-threshold -90
 action log
nx9500-6C8809(config-roaming-assist-policy-test)#
```

## Related Commands

|                              |                                                    |
|------------------------------|----------------------------------------------------|
| <code>no</code> on page 1850 | Removes the configured detection threshold details |
|------------------------------|----------------------------------------------------|

## *disassoc-time*

Configures the disassociation time. This is the interval after which a disassociation message is sent.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

## Syntax

```
disassoc-time <1-10>
```

## Parameters

```
disassoc-time <1-10>
```

|                                         |                                                                                                                                                                               |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>disassoc-time &lt;1-10&gt;</code> | Configures the disassociation time in seconds <ul style="list-style-type: none"><li>• &lt;1-10&gt; - Specify a value from 1 - 10 seconds. The default is 5 seconds.</li></ul> |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-roaming-assist-policy-test)#disassoc-time 7
nx9500-6C8809(config-roaming-assist-policy-test)#show context
roaming-assist-policy test
 aggressiveness medium-high
 detection-threshold -90
 action log
 disassoc-time 7
nx9500-6C8809(config-roaming-assist-policy-test)#
```

## Related Commands

|                              |                                            |
|------------------------------|--------------------------------------------|
| <code>no</code> on page 1850 | Removes the configured disassociation time |
|------------------------------|--------------------------------------------|

## *handoff-count*

Specifies the number of times a client can exceed the specified handoff-threshold value before an action is invoked

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
handoff-count <1-10>
```

### Parameters

```
handoff-count <1-10>
```

|                      |                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| handoff-count <1-10> | Specifies the number of times a client can exceed the specified handoff-threshold value before an action is invoked <ul style="list-style-type: none"><li>• &lt;1-10&gt; – Specify a value from 1 - 10. The default is 3.</li></ul> If the client's RSSI increases beyond the set handoff-threshold, it is removed from the queue for monitoring and action invocation. |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config-roaming-assist-policy-test)#handoff-count 5
nx9500-6C8809(config-roaming-assist-policy-test)#show context
roaming-assist-policy test
 aggressiveness medium-high
 handoff-count 5
 detection-threshold -90
 action log
 disassoc-time 7
nx9500-6C8809(config-roaming-assist-policy-test)#
```

### Related Commands

|                              |                                                 |
|------------------------------|-------------------------------------------------|
| <code>no</code> on page 1850 | Reverts the configured handoff-count to default |
|------------------------------|-------------------------------------------------|

### *handoff-threshold*

Configures the handoff-threshold, which specifies client status for handoff-action. Once exceeded an action is invoked.

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
handoff-threshold <-100--40>
```

### Parameters

```
handoff-threshold <-100--40>
```

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| handoff-threshold<br><-100--40> | <p>Configures the handoff-threshold, which specifies client status for handoff-action. Once exceeded an action is invoked.</p> <ul style="list-style-type: none"> <li>• &lt;-100--40&gt; - Specify the RSSI value from -100 dBm - -40 dBm. The default is -80 dBm.</li> </ul> <p>If the client's RSSI increases beyond the set handoff-threshold, it is removed from the queue for monitoring and action invocation.</p> |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```

nx9500-6C8809(config-roaming-assist-policy-test)#handoff-threshold -75
nx9500-6C8809(config-roaming-assist-policy-test)#show context
roaming-assist-policy test
 aggressiveness medium-high
 handoff-count 5
 detection-threshold -90
 handoff-threshold -75
 action log
 disassoc-time 7
nx9500-6C8809(config-roaming-assist-policy-test)#

```

### Related Commands

|                 |                                                  |
|-----------------|--------------------------------------------------|
| no on page 1850 | Removes the configured handoff-threshold details |
|-----------------|--------------------------------------------------|

### *monitoring-interval*

Configures the interval, in seconds, at which clients are monitored to determine if their RSSI value is below the specified handoff-threshold value

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
monitoring-interval <1-60>
```

### Parameters

```
monitoring-interval <1-60>
```

|                               |                                                                                                                                                                                                                                                                                      |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| monitoring-interval<br><1-60> | <p>Specifies the interval, in seconds, at which clients are monitored to determine if their RSSI is below the specified handoff-threshold</p> <ul style="list-style-type: none"> <li>• &lt;1-60&gt; - Specify the duration from 1 - 60 seconds. The default is 5 seconds.</li> </ul> |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```

nx9500-6C8809(config-roaming-assist-policy-test)#monitoring-interval 40
nx9500-6C8809(config-roaming-assist-policy-test)#show context
roaming-assist-policy test
 aggressiveness medium-high
 monitoring-interval 40
 handoff-count 5
 detection-threshold -90
 handoff-threshold -75

```

```
action log
disassoc-time 7
nx9500-6C8809(config-roaming-assist-policy-test)#
```

### Related Commands

|                              |                                                    |
|------------------------------|----------------------------------------------------|
| <code>no</code> on page 1850 | Removes the configured monitoring interval details |
|------------------------------|----------------------------------------------------|

### *sampling interval*

Configures the interval, in seconds, at which clients are sampled to determine their RSSI value

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
sampling-interval <5-60>
```

### Parameters

```
sampling-interval <5-60>
```

|                                             |                                                                                                                                                                                                                                  |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>sampling-interval &lt;5-60&gt;</code> | Configures the interval, in seconds, between two successive client samplings <ul style="list-style-type: none"><li>• <code>&lt;5-60&gt;</code> – Specify a value from 5 - 60 seconds. The default value is 15 seconds.</li></ul> |
|                                             | <b>Note:</b> Higher the RSSI number, stronger is the signal.                                                                                                                                                                     |

### Examples

```
nx9500-6C8809(config-roaming-assist-policy-test)#sampling-interval 10
nx9500-6C8809(config-roaming-assist-policy-test)#show context
roaming-assist-policy test
 aggressiveness medium-high
 sampling-interval 10
 monitoring-interval 40
 handoff-count 5
 detection-threshold -90
 handoff-threshold -75
 action log
 disassoc-time 7
nx9500-6C8809(config-roaming-assist-policy-test)#
```

### Related Commands

|                              |                                                  |
|------------------------------|--------------------------------------------------|
| <code>no</code> on page 1850 | Removes the configured sampling interval details |
|------------------------------|--------------------------------------------------|

### *no*

Removes or reverts this roaming assist policy settings based on the parameters passed

### Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

### Syntax

```
no [action|aggressiveness|detection-threshold|disassoc-time|handoff-count |
handoff-threshold|monitoring-interval|sampling-interval]
```

### Parameters

```
no <PARAMETERS>
```

|                                                                                                                  |
|------------------------------------------------------------------------------------------------------------------|
| no <PARAMETERS> Removes or reverts this roaming assist policy settings to default based on the parameters passed |
|------------------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config-roaming-assist-policy-test)#show context
roaming-assist-policy test
 aggressiveness medium-high
 sampling-interval 10
 monitoring-interval 40
 handoff-count 5
 detection-threshold -90
 handoff-threshold -75
 action log
 disassoc-time 7
nx9500-6C8809(config-roaming-assist-policy-test)#
nx9500-6C8809(config-roaming-assist-policy-test)#no action
nx9500-6C8809(config-roaming-assist-policy-test)#no detection-threshold
nx9500-6C8809(config-roaming-assist-policy-test)#no handoff-threshold
nx9500-6C8809(config-roaming-assist-policy-test)#show context
roaming-assist-policy test
 aggressiveness medium-high
 sampling-interval 10
 monitoring-interval 40
 handoff-count 5
 disassoc-time 7
nx9500-6C8809(config-roaming-assist-policy-test)#
```

# BORDER GATEWAY PROTOCOL

## BORDER GATEWAY PROTOCOL

---

This chapter summarizes the BGP (Border Gateway Protocol) related configuration commands in the CLI command structure.

BGP is a routing protocol, which establishes routing between ISPs. ISPs use BGP to exchange routing information between ASs (Autonomous Systems) on the Internet. The routing information shared includes details, such as ASs traversed to a particular destination, reachable ASs, best paths available, network policies and rules applied on a route, etc. These details appear as BGP attributes carried in routing update packets. BGP uses this information to make routing decisions. Therefore, the primary role of a BGP system is to exchange routing information with other BGP peers.

BGP uses TCP as its transport protocol. This eliminates the need to implement explicit update fragmentation, retransmission, acknowledgement, and sequencing. BGP listens on TCP port 179. The error notification mechanism used in BGP assumes that TCP supports a graceful close (all outstanding data is delivered before the connection is closed). Routing information exchanged through BGP supports only destination-based forwarding (it assumes a router forwards packets based on the destination address carried in the IP header of the packet).

An AS is a set of routers under the same administration that use Interior Gateway Protocol (IGP) and common metrics to define how to route packets within the AS. There are two types of BGP systems: eBGP (external BGP) and iBGP (internal BGP). iBGP represents the exchange of routing information between BGP peers within an AS. Whereas, when two BGP peers, belonging to different ASs, are connected you have an eBGP setup.

BGP peers (also referred to as neighbors) are BGP enabled devices that are directly connected through an established TCP connection. When two BGP enabled peers establish a TCP connection the first time, they exchange their BGP routing tables. All subsequent route table modifications are exchanged as route updates. BGP tracks these route updates by maintaining route table version numbers. With every update the version number changes. At any given point in time, all BGP peers should have the same route table version. The peer-to-peer TCP connections are kept alive through keepalive packets exchanged at specified intervals. Errors and special events are communicated between peers as notification packets.



### Note

The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (\_) character. In other words, the name of a device cannot contain an underscore.

---

## bgp ip-prefix-list

IP prefix lists are a convenient way to filter prefixes (contained in route update packets) transmitted to (or received from) other BGP supported routers. IP prefix lists are similar to access lists. They contain ordered entries (deny or permit prefix rules), identified by their sequence numbers. Each rule specifies



match criteria (network and subnet prefixes and prefix masks) to match. When a prefix (received or transmitted) matches the prefix specified in one of the rules, it is filtered and an action is applied depending on where the IP prefix list is used. For example, when used in the BGP neighbor context, the prefixes received from the neighbor are filtered and the filtered prefixes are either rejected or accepted depending on the rule type (deny or permit).

IP prefix lists are also used in the BGP route map context to filter prefixes. The action applied, on filtered prefixes is set within the route map. Another use case for IP prefix lists is to filter prefixes before redistribution of local OSPF routes to eBGP enabled ASs.

Like in access lists, these deny and permit prefix rules are processed sequentially, in ascending order of their sequence number. Once a match is made, the BGP enabled router stops processing all subsequent rules in the ip-prefix-list.

IP prefix lists are used as match criteria in the following contexts:

- BGP neighbor. For more information, see [use](#).
- BGP route-map context. For more information, see [match](#).

To navigate to the ip-prefix-list configuration instance, use the following command:

```
<DEVICE>(config)#bgp ip-prefix-list <IP-PREFIX-LIST-NAME>
<DEVICE>(config-bgp-ip-prefix-list-test)#?
BGP IP Prefix List Mode commands:
 deny IP Prefix deny rule to specify packets to reject
 no Negate a command or set its defaults
 permit IP Prefix permit rule to specify packets to forward

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

<DEVICE>(config-bgp-ip-prefix-list-test)#
```

The following table summarizes the BGP IP prefix list configuration commands:

**Table 69: BGP IP-Prefix-List Config Mode Commands**

| Command                                              | Description                                                                    |
|------------------------------------------------------|--------------------------------------------------------------------------------|
| <a href="#">deny (ip-prefix-list)</a> on page 1853   | Creates and configures a deny, prefix-list rule                                |
| <a href="#">permit (ip-prefix-list)</a> on page 1854 | Creates and configures a permit, prefix-list rule                              |
| <a href="#">no (ip-prefix-list)</a> on page 1855     | Removes the specified deny or permit prefix-list rule from this IP prefix list |

### *deny (ip-prefix-list)*

Creates and configures a deny prefix-list rule. The deny rule specifies match criteria based on which prefixes received from (or transmitted to) a BGP neighbor are filtered. A deny action is applied on these filtered prefixes. For example, in the BGP router neighbor context a filter is applied using a IP prefix list.

The list contains a deny rule with a prefix to match as 192.168.13.0/24. All prefixes received from the neighbor matching this prefix are denied.

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

### Syntax

```
deny prefix-list <1-4292967294> [<PREFIX-TO-MATCH/MASK>|any]
deny prefix-list <1-4292967294> [<PREFIX-TO-MATCH/MASK> {ge <0-32>/le <0-32>}|any]
```

### Parameters

```
deny prefix-list <1-4292967294> [<PREFIX-TO-MATCH/MASK> {ge <0-32>/le <0-32>}|any]
```

|                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>deny prefix-list &lt;1-4294967295&gt; [&lt;PREFIX-TO-MATCH/MASK&gt; any]</pre> | <p>Creates and configures a deny prefix-list rule</p> <ul style="list-style-type: none"><li>• &lt;1-4294967295&gt; - Configures a sequence number for this deny rule. Specify a value from 1 - 4294967295. Within a prefix list, rules are applied in an ascending order of their sequence number. Rules with lower sequence number are applied first.</li><li>• &lt;PREFIX-TO-MATCH/MASK&gt; - Specify the prefix to match. For example 10.0.0.0/8 or 192.168.13.0/24. Routes matching the specified prefix are filtered.<ul style="list-style-type: none"><li>ge &lt;0-32&gt; - Optional. Specifies a greater than or equal to value for the IP prefix length (subnet mask)</li><li>le &lt;0-32&gt; - Optional. Specifies a less than or equal to value for the IP prefix length</li></ul></li></ul> <p>The 'ge' and 'le' options specify a IP prefix length range. Use these options to specify a more specific (granular) prefix match criteria.</p> <ul style="list-style-type: none"><li>any - Sets the prefix match criteria to any. When selected, all routes are filtered, and the action applied is deny. At the backend, this option sets the match criteria to 0.0.0.0/0 le 32.</li></ul> |
|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config-bgp-ip-prefix-list-test)#deny prefix-list 1 168.192.13.0/24
nx9500-6C8809(config-bgp-ip-prefix-list-test)#show context
bgp ip-prefix-list test
 deny prefix-list 1 168.192.13.0/24
nx9500-6C8809(config-bgp-ip-prefix-list-test)#
```

### Related Commands

|                                |              |                                                              |
|--------------------------------|--------------|--------------------------------------------------------------|
| <pre>no (ip-prefix-list)</pre> | on page 1855 | Removes a deny, ip-prefix-list rule from this IP prefix list |
|--------------------------------|--------------|--------------------------------------------------------------|

### *permit (ip-prefix-list)*

Creates and configures a permit prefix-list rule. The permit rule specifies match criteria based on which prefixes received from (or transmitted to) a BGP neighbor are filtered. A permit action is applied on these filtered prefixes. For example, in the BGP router neighbor context a filter is applied using a IP

prefix list. The list contains a permit rule with a prefix to match as 172.168.10.0/24. All prefixes received from the neighbor matching this prefix are permitted.

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

### Syntax

```
permit prefix-list <1-4294967295> [<PREFIX-TO-MATCH/MASK>|any]
```

### Parameters

```
permit prefix-list <1-4294967295> [<PREFIX-TO-MATCH/MASK>|any]
```

|                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>deny prefix-list &lt;1-4294967295&gt; [&lt;PREFIX-TO-MATCH/MASK&gt; any]</pre> | <p>Creates and configures a permit prefix-list rule</p> <ul style="list-style-type: none"><li>• &lt;1-4294967295&gt; - Configures a sequence number for this permit rule. Specify a value from 1 - 4294967295. Within a prefix list, rules are applied in an ascending order of their sequence number. Rules with lower sequence number are applied first.</li><li>• &lt;PREFIX-TO-MATCH/MASK&gt; - Specify the prefix to match. For example 10.0.0.0/8 or 192.168.13.0/24. Routes matching the specified prefix are filtered.<ul style="list-style-type: none"><li>ge - Optional. Specifies a greater than or equal to value for the IP prefix length (subnet mask)</li><li>le - Optional. Specifies a less than or equal to value for the IP prefix length</li></ul></li></ul> <p>Use the 'ge' and 'le' options to specify a IP prefix length range. Use these options to specify a more specific (granular) prefix match criteria.</p> <ul style="list-style-type: none"><li>• any - Sets the prefix match criteria to any. When selected, all routes are filtered, and the action applied is permit. At the backend, this option sets the match criteria to 0.0.0.0/0 le 32.</li></ul> |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config-bgp-ip-prefix-list-test)#permit prefix-list 2 172.122.10.0/24
nx9500-6C8809(config-bgp-ip-prefix-list-test)#show context
bgp ip-prefix-list test
 deny prefix-list 1 168.192.13.0/24
 permit prefix-list 2 172.122.10.0/24
nx9500-6C8809(config-bgp-ip-prefix-list-test)#
```

### Related Commands

|                                               |                                                                |
|-----------------------------------------------|----------------------------------------------------------------|
| <code>no (ip-prefix-list)</code> on page 1855 | Removes a permit, ip-prefix-list rule from this IP prefix list |
|-----------------------------------------------|----------------------------------------------------------------|

*no (ip-prefix-list)*

Removes the specified deny or permit prefix-list rule from this IP prefix list

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

## Syntax

```
no [deny|permit]
no [deny|permit] prefix-list <1-4294967295> {<PREFIX-TO-MATCH/MASK>|any}
```

## Parameters

```
no <PARAMETERS>
```

|                 |                                                        |
|-----------------|--------------------------------------------------------|
| no <PARAMETERS> | Removes a deny or permit rule from this IP prefix list |
|-----------------|--------------------------------------------------------|

## Examples

The following example shows the IP prefix list 'test' settings before the 'no' command is executed:

```
nx9500-6C8809(config-bgp-ip-prefix-list-test)#show context
bgp ip-prefix-list test
 deny prefix-list 1 168.192.13.0/24
 permit prefix-list 2 172.122.10.0/24
nx9500-6C8809(config-bgp-ip-prefix-list-test)#
```

The following example shows the IP prefix list 'test' settings after the 'no' command is executed:

```
nx9500-6C8809(config-bgp-ip-prefix-list-test)#no deny prefix-list 1 168.192.13.0/24
nx9500-6C8809(config-bgp-ip-prefix-list-test)#show context
bgp ip-prefix-list test
 permit prefix-list 2 172.122.10.0/24
nx9500-6C8809(config-bgp-ip-prefix-list-test)#
```

## bgp ip-access-list

BGP peers and route maps can reference a single IP based ACL (access control list). Apply IP ACLs to both inbound and outbound route updates. When applied to a BGP enabled router, every route update is passed through the ACL. Each ACL contains deny and permit entries that are applied sequentially, in the order they appear within the list. When a route matches an entry, the decision to permit or deny the route is applied. Once a match is made the remaining entries in the ACL are not processed.

BGP IP ACLs are used as match criteria in the following contexts:

- BGP neighbor. For more information, see [use](#).
- BGP route-map context. For more information, see [match](#).

To navigate to the BGP IP ACL configuration instance, use the following command:

```
<DEVICE>(config)#bgp ip-access-list <IP-ACL-NAME>
<DEVICE>(config-bgp-ip-access-list-<IP-ACL-NAME>)#?
BGP IP Access List Mode commands:
 deny Specify packets to reject
 no Negate a command or set its defaults
 permit Specify packets to forward

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

<DEVICE>(config-bgp-ip-access-list-<IP-ACL-NAME>)#
```

The following table summarizes the BGP IP access list configuration commands:

**Table 70: BGP IP-Access-List Config Mode Commands**

| Command                                               | Description                                                  |
|-------------------------------------------------------|--------------------------------------------------------------|
| <code>deny (bgp-ip-access-list)</code> on page 1857   | Creates and configures a deny entry rule for this BGP IP ACL |
| <code>permit (bgp-ip-access-list)</code> on page 1857 | Creates and configures a permit entry for this BGP IP ACL    |
| <code>no (bgp-ip-access-list)</code> on page 1858     | Removes a deny or permit entry from this BGP IP ACL          |

### *deny (bgp-ip-access-list)*

Creates and configures a deny entry for this BGP IP ACL

#### **Supported in the following platforms:**

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

#### **Syntax**

```
deny access-list [<PREFIX-TO-MATCH/MASK> {exact-match}|any]
```

#### **Parameters**

```
deny access-list [<PREFIX-TO-MATCH/MASK> {exact-match}|any]
```

|                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>deny access-list [&lt;PREFIX-TO-MATCH/MASK&gt; {exact-match} any]</code> | <p>Creates and configures a deny entry for this BGP IP ACL</p> <ul style="list-style-type: none"><li>• <code>&lt;PREFIX-TO-MATCH/MASK&gt;</code> - Specify the prefix to match.<ul style="list-style-type: none"><li>• <code>exact-match</code> - Optional. Enables an exact match of the prefix provided in the previous step. When configured, the route is denied only in case of an exact match.</li></ul></li><li>• <code>any</code> - Specifies the prefix to match as 'any'.</li></ul> |
|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### **Examples**

```
nx9500-6C8809(config-bgp-ip-access-list-test)#deny access-list 192.168.13.0/24 exact-match
nx9500-6C8809(config-bgp-ip-access-list-test)#show context
bgp ip-access-list test
 deny access-list 192.168.13.0/24 exact-match
nx9500-6C8809(config-bgp-ip-access-list-test)#
```

#### **Related Commands**

|                                                   |                                                         |
|---------------------------------------------------|---------------------------------------------------------|
| <code>no (bgp-ip-access-list)</code> on page 1858 | Removes the specified the deny entry in this IP BGP ACL |
|---------------------------------------------------|---------------------------------------------------------|

### *permit (bgp-ip-access-list)*

Creates and configures a permit entry for this BGP IP ACL

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

### Syntax

```
permit access-list [<PREFIX-TO-MATCH/MASK> {exact-match}|any]
```

### Parameters

```
permit access-list [<PREFIX-TO-MATCH/MASK> {exact-match}|any]
```

|                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| permit access-list [<PREFIX-TO-MATCH/MASK> {exact-match} any] | Creates and configures a permit entry for this BGP IP ACL <ul style="list-style-type: none"><li>• &lt;PREFIX-TO-MATCH/MASK&gt; - Specify the prefix to match.<ul style="list-style-type: none"><li>• exact-match - Optional. Enables an exact match of the prefix provided in the previous step. When configured, the route is permitted only in case of an exact match.</li><li>• any - Specifies the prefix to match as 'any'.</li></ul></li></ul> |
|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config-bgp-ip-access-list-test)#permit access-list 172.168.10.0/24
nx9500-6C8809(config-bgp-ip-access-list-test)#show context
bgp ip-access-list test
 permit access-list 172.168.10.0/24
 deny access-list 192.168.13.0/24 exact-match
nx9500-6C8809(config-bgp-ip-access-list-test)#
```

### Related Commands

|                                                      |                                                           |
|------------------------------------------------------|-----------------------------------------------------------|
| <a href="#">no (bgp-ip-access-list)</a> on page 1858 | Removes the specified the permit entry in this IP BGP ACL |
|------------------------------------------------------|-----------------------------------------------------------|

*no (bgp-ip-access-list)*

Removes a deny or permit entry from this BGP IP ACL

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

### Syntax

```
no [deny|permit]
no [deny|permit] access-list [<PREFIX-TO-MATCH/MASK>|any]
```

### Parameters

```
no <PARAMETERS>
```

|                 |                                                     |
|-----------------|-----------------------------------------------------|
| no <PARAMETERS> | Removes a deny or permit entry from this BGP IP ACL |
|-----------------|-----------------------------------------------------|

## Examples

The following example shows the BGP IP ACL 'test' settings before the 'no' command is executed:

```
nx9500-6C8809(config-bgp-ip-access-list-test)#show context
bgp ip-access-list test
 permit access-list 172.168.10.0/24
 deny access-list 192.168.13.0/24 exact-match
nx9500-6C8809(config-bgp-ip-access-list-test)#
nx9500-6C8809(config-bgp-ip-access-list-test)#no permit access-list 172.168.10.0/24
```

The following example shows the BGP IP ACL 'test' settings after the 'no' command is executed:

```
nx9500-6C8809(config-bgp-ip-access-list-test)#show context
bgp ip-access-list test
 deny access-list 192.168.13.0/24 exact-match
nx9500-6C8809(config-bgp-ip-access-list-test)#
```

## bgp as-path-list

BGP enabled devices use routing updates to exchange network routing information with each other. This information includes route details, such as the network number, path specific attributes, and the list of ASNs (Autonomous System Numbers) that a route traverses to reach a destination. This list is contained in the AS path.

An AS path ACL (access control list) filters AS paths (routes) included in routing updates. Each AS path access list consists of deny and/or permit rules that define regular expressions (match criteria). When configured and applied on inbound and outbound routing updates, the BGP AS path attributes are matched against the regular expressions specified in the AS path ACL. In case of a match, the route is filtered and an action (deny or permit) is applied. Once a match is made subsequent rules in the AS path access list are not processed.

AS path access lists also help prevent looping within an AS. Routing loops are prevented by rejecting routing updates containing local ASNs. Since local ASNs indicate that the route has already traveled through that autonomous system, by rejecting them looping is avoided.

AS path access lists are used as match criteria in the following contexts:

- BGP neighbor. For more information, see [use](#).
- BGP route map context. For more information, see [match](#).

To navigate to the AS path configuration instance, use the following command:

```
<DEVICE>(config)#bgp as-path <AS-PATH-LIST-NAME>
<DEVICE>(config-bgp-as-path-list-<AS-PATH-LIST-NAME>)#?
BGP AS Path List Mode commands:
deny Specify packets to reject
no Negate a command or set its defaults
permit Specify packets to forward

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal
```

```
<DEVICE>(config-bgp-as-path-list-<AS-PATH-LIST-NAME>)#
```

The following table summarizes the BGP AS path list configuration commands:

**Table 71: BGP AS-Path-List Config Mode Commands**

| Command                                             | Description                                         |
|-----------------------------------------------------|-----------------------------------------------------|
| <code>deny (bgp-as-path-list)</code> on page 1860   | Creates and configures a deny as-path-list rule     |
| <code>permit (bgp-as-path-list)</code> on page 1861 | Creates and configures a permit as-path-list rule   |
| <code>no (bgp-as-path-list)</code> on page 1862     | Removes a deny or permit rule from this AS path ACL |

### *deny (bgp-as-path-list)*

Creates and configures a deny as-path-list rule. The deny rule specifies a regular expression to match. This regular expression, is matched against the BGP AS paths contained in routing updates. AS paths matching the provided string are filtered and a deny action is applied.

#### **Supported in the following platforms:**

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

#### **Syntax**

```
deny as-path <REG-EXP>
```

#### **Parameters**

```
deny as-path <REG-EXP>
```

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| deny as-path <REG-EXP> | Configures a match criteria (regular expression). <ul style="list-style-type: none"><li>• &lt;REG-EXP&gt; – Specify the regular expression to match (should not exceed 64 characters and should be unique to the AS path list rule)</li></ul> Regular expressions are treated as a 'ASCII string' and not as a sequence of numbers. Create a regular expression ideally suited to filter the required AS paths. |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### **Usage Guidelines**

The following table lists some of the characters used in forming regular expressions:

**Table 72:**

| Character to use | Description                                                                                                   |
|------------------|---------------------------------------------------------------------------------------------------------------|
| ^                | Indicates the start of a string                                                                               |
| \$               | Indicates the end of a string                                                                                 |
| _ (underscore)   | Indicates a comma, left brace, right brace, start and end of an input string, or a space. For example, “_ _”. |



## Examples

```
nx9500-6C8809(config-bgp-as-path-list-test)#deny as-path ^100$
nx9500-6C8809(config-bgp-as-path-list-test)#show context
bgp as-path-list test
 deny as-path ^100$
nx9500-6C8809(config-bgp-as-path-list-test)#
```

## Related Commands

|                                                 |                                          |
|-------------------------------------------------|------------------------------------------|
| <code>no (bgp-as-path-list)</code> on page 1862 | Removes the specified deny, as-path rule |
|-------------------------------------------------|------------------------------------------|

### *permit (bgp-as-path-list)*

Creates and configures a permit as-path-list rule. The permit rule specifies a regular expression to match. This regular expression is matched against the BGP AS paths contained in routing updates. AS paths matching the provided string are filtered and a permit action is applied.

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

### Syntax

```
permit as-path <REG-EXP>
```

### Parameters

```
permit as-path <REG-EXP>
```

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| permit as-path <REG-EXP> | Configures a match criteria (regular expression). <ul style="list-style-type: none"><li>• &lt;REG-EXP&gt; - Specify the regular expression to match (should not exceed 64 characters and should be unique to the AS path list rule)</li></ul> Regular expressions are treated as a 'ASCII string' and not as a sequence of numbers. Create a regular expression which is ideally suited to filter the required AS paths. |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Usage Guidelines

The following table lists some of the characters used in forming regular expressions:

**Table 73:**

| Character to use | Description                                                                                                   |
|------------------|---------------------------------------------------------------------------------------------------------------|
| ^                | Indicates the start of a string                                                                               |
| \$               | Indicates the end of a string                                                                                 |
| _ (underscore)   | Indicates a comma, left brace, right brace, start and end of an input string, or a space. For example, “_ _”. |

### Examples

```
nx9500-6C8809(config-bgp-as-path-list-test)#permit as-path _200_
nx9500-6C8809(config-bgp-as-path-list-test)#permit as-path _323_
nx9500-6C8809(config-bgp-as-path-list-test)#show context
bgp as-path-list test
```

```
deny as-path ^100$
permit as-path _323_
permit as-path _200_
nx9500-6C8809(config-bgp-as-path-list-test)#
```

### Related Commands

|                                                 |                                               |
|-------------------------------------------------|-----------------------------------------------|
| <code>no (bgp-as-path-list)</code> on page 1862 | Removes the specified permit as-path ACL rule |
|-------------------------------------------------|-----------------------------------------------|

*no (bgp-as-path-list)*

Removes a deny or permit rule from this AS path ACL

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

### Syntax

```
no as-path-list [deny|permit] <REG-EXP>
```

### Parameters

```
no <PARAMETERS>
```

|                                    |                                                     |
|------------------------------------|-----------------------------------------------------|
| <code>no &lt;PARAMETERS&gt;</code> | Removes a deny or permit rule from this AS path ACL |
|------------------------------------|-----------------------------------------------------|

### Examples

The following example shows the BGP As-Path-List 'test' configuration before the 'no' command is executed:

```
nx9500-6C8809(config-bgp-as-path-list-test)#show context
bgp as-path-list test
 deny as-path ^100$
 permit as-path _323_
 permit as-path _200_
nx9500-6C8809(config-bgp-as-path-list-test)#
nx9500-6C8809(config-bgp-as-path-list-test)#no permit as-path _323_
```

The following example shows the BGP As-Path-List 'test' configuration after the 'no' command is executed:

```
nx9500-6C8809(config-bgp-as-path-list-test)#show context
bgp as-path-list test
 deny as-path ^100$
 permit as-path _200_
nx9500-6C8809(config-bgp-as-path-list-test)#
```

## bgp community-list

Creates and configures a named community list

IP BGP routes have a set of attributes, mandatory and optional. The community and extended community attributes are optional. Optional attributes are specified by network administrators to mark (color) routes received in updates containing these attributes. These marked routes are filtered and special actions applied (accepted, preferred, distributed, or advertised). For example, the NO\_EXPORT

community, indicates that routes attached to it are local and not to be advertised to external ASs. Similarly, a set of routes using a common routing policy can be tagged to a community, and the policy applied to the community.

A BGP community is a group of routes sharing common attributes. Route updates contain community information in the form of path attributes. These attributes help identify community members.

A BGP community list is a list of deny or permit entries. It is either assigned a name (regular expressions, predefined community names) or a number. Assigning names to communities increases the number of configurable community lists. All rules applicable to numbered communities apply to named communities too. The only difference being in the number of attributes configurable for a named community list.

Since the community attribute is optional, it is shared only between devices that understand communities and are configured to handle communities. By default the community attribute is not sent to neighbors unless the `send-community` command option is enabled in the BGP neighbor context. For more information, see [send-community](#).

Some of the predefined, globally used communities are:

- no-export – Routes tagged to this community are not advertised to external BGP peers
- no-advertise – Routes tagged to this community are not advertised to any BGP peers
- local-as – Routes tagged to this community are not advertised outside the local AS
- internet – Routes tagged to this community are advertised to the Internet community. By default all BGP enabled devices belong to this community.

BGP community lists are used in the following context as match clauses:

- BGP route map context. For more information, see [match](#).

To navigate to the BGP community configuration instance, use the following command:

```
<DEVICE>(config)#bgp community-list <COMMUNITY-LIST-NAME>
<DEVICE>(config-bgp-community-list-<COMMUNITY-LIST-NAME>)#?
BGP Community List Mode commands:
deny Add a BGP Community List deny rule to Specify community to reject
no Negate a command or set its defaults
permit Add a BGP Community List permit rule to Specify community to accept

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

<DEVICE>(config-bgp-community-list-<COMMUNITY-LIST-NAME>)#
```

The following table summarizes the BGP community list configuration commands:

**Table 74: BGP Community-List Config Mode Commands**

| Command                                               | Description                                                                |
|-------------------------------------------------------|----------------------------------------------------------------------------|
| <code>deny (bgp-community-list)</code> on page 1864   | Creates and configures a deny community (expanded or standard) rule        |
| <code>permit (bgp-community-list)</code> on page 1865 | Creates and configures a permit community (expanded or standard) rule      |
| <code>no (bgp-community-list)</code> on page 1866     | Removes an existing deny or permit community rule from this community list |

### *deny (bgp-community-list)*

Creates and configures a deny community (expanded or standard) rule

#### **Supported in the following platforms:**

- Wireless Controllers – RFS 4000
- Service Platforms – NX 95XX, NX 96XX

#### **Syntax**

```
deny community [expanded|standard]
deny community expanded <LINE>
deny community standard [AA:NN|internet|local-AS|no-advertise|no-export]
```

#### **Parameters**

```
deny community expanded <LINE>
```

|                                                   |                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>deny community expanded &lt;LINE&gt;</code> | <p>Configures a deny expanded community list entry and associates it with a regular expression to match. The regular expression represents the patterns to match in the community attributes.</p> <ul style="list-style-type: none"> <li>• &lt;LINE&gt; - Provide the regular expression.</li> </ul> |
|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
deny community standard [AA:NN|internet|local-AS|no-advertise|no-export]
```

|                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>deny community standard [AA:NN internet local-AS no-advertise no-export]</code> | <p>Configures a deny standard community list entry and associates it with a predefined, globally used, known community or community number. The options are:</p> <ul style="list-style-type: none"> <li>• aa:nn - Configures the community number. The first part (aa) represents the AS number. The second part (nn) represents a 2-byte number.</li> <li>• internet - Advertises this route to the internet community</li> <li>• local-AS - Prevents transmission of this route outside the local AS</li> <li>• no-advertise - Prevents advertisement of this route to any peer (internal or external)</li> <li>• no-export - Prevents advertisement of this route to external BGP peers (keeping this route within an AS)</li> </ul> |
|---------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-bgp-community-list-test)#deny community expanded 100
nx9500-6C8809(config-bgp-community-list-test)#show context
bgp community-list test
 deny community expanded 100
nx9500-6C8809(config-bgp-community-list-test)#
```

## Related Commands

|                                                   |                                                                        |
|---------------------------------------------------|------------------------------------------------------------------------|
| <code>no (bgp-community-list)</code> on page 1866 | Removes the specified deny community rule from this BGP community list |
|---------------------------------------------------|------------------------------------------------------------------------|

## *permit (bgp-community-list)*

Creates and configures a permit community (expanded or standard) rule

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

### Syntax

```
permit community [expanded|standard]
permit community expanded <LINE>
permit community standard [AA:NN|internet|local-AS|no-advertise|no-export]
```

### Parameters

```
permit community expanded <LINE>
```

|                                                     |                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>permit community expanded &lt;LINE&gt;</code> | Configures a permit expanded community list entry and associates it with a regular expression to match. The regular expression represents the patterns to match in the community attributes. <ul style="list-style-type: none"><li>• &lt;LINE&gt; - Provide the regular expression.</li></ul> |
|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
permit community standard [AA:NN|internet|local-AS|no-advertise|no-export]
```

|                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>permit community standard [AA:NN internet local-AS no-advertise no-export]</code> | Configures a permit standard community list entry and associates it with a predefined, globally used, known community or community number. The options are: <ul style="list-style-type: none"><li>• aa:nn - Configures the community number. The first part (aa) represents the AS number. The second part (nn) represents a 2-byte number.</li><li>• internet - Advertises this route to the internet community</li><li>• local-AS - Allows transmission of this route outside the local AS</li><li>• no-advertise - Allows advertisement of this route to any peer (internal or external)</li><li>• no-export - Allows advertisement of this route to external BGP peers (keeping this route within an AS)</li></ul> |
|-----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-bgp-community-list-test)#permit community expanded 300
nx9500-6C8809(config-bgp-community-list-test)# show context
bgp community-list test
 permit community expanded 300
 deny community expanded 100
nx9500-6C8809(config-bgp-community-list-test)#
nx9500-6C8809(config-bgp-community-list-test1)#permit community standard no-export
nx9500-6C8809(config-bgp-community-list-test1)#show context
bgp community-list test1
 permit community standard no-export
nx9500-6C8809(config-bgp-community-list-test1)#
```

## Related Commands

|                                                   |                                                                      |
|---------------------------------------------------|----------------------------------------------------------------------|
| <code>no (bgp-community-list)</code> on page 1866 | Removes the specified permit community rule from this community list |
|---------------------------------------------------|----------------------------------------------------------------------|

### *no (bgp-community-list)*

Removes a deny or permit community rule from this community list

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

### Syntax

```
no [deny|permit] community expanded <LINE>
no [deny|permit] community standard [AA:NN|internet|local-AS|no-advertise|no-export]
```

### Parameters

no <PARAMETERS>

|                                    |                                                                                                                                                                                                     |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>no &lt;PARAMETERS&gt;</code> | Removes a deny or permit expanded community rule from this community list <ul style="list-style-type: none"><li>• &lt;LINE&gt; - Specify the regular expression associated with the rule.</li></ul> |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

The following example shows the settings of the community list 'test' before the 'no' command is executed:

```
nx9500-6C8809(config-bgp-community-list-test)#show context
bgp community-list test
 permit community expanded 300
 deny community expanded 100
nx9500-6C8809(config-bgp-community-list-test)#
nx9500-6C8809(config-bgp-community-list-test)#no deny community expanded 100
```

The following example shows the settings of the community list 'test' after the 'no' command is executed:

```
nx9500-6C8809(config-bgp-community-list-test)#show context
bgp community-list test
 permit community expanded 300
nx9500-6C8809(config-bgp-community-list-test)#
```

## bop ext-community-list

Creates and configures a named extended community list

A BGP extended community is a group of routes sharing a common attribute, regardless of their network or physical boundary. By using a BGP extended community attribute, routing policies can implement inbound or outbound route filters based on the extended community tag, rather than a long list of individual permit or deny rules. A BGP extended community list is used to create groups of communities to use in a match clause of a route map. An extended community list is used to control which routes are accepted, preferred, distributed, or advertised.

The BGP extended community and standard community attributes are identical in function and structure, except that the former is an eight octet and the latter is a four octet attribute.

BGP extended community lists are used as match clauses in the following context:

- BGP route map context. For more information, see [match](#).

To navigate to the extended community configuration instance, use the following command:

```
<DEVICE>(config)#bgp extcommunity-list <EXTCOMMUNITY-LIST-NAME>
<DEVICE>(config-bgp-extcommunity-list-<EXTCOMMUNITY-LIST-NAME>)#?
BGP Extcommunity List Mode commands:
 deny Add a BGP Community List deny rule to specify extcommunity to
 reject
 no Negate a command or set its defaults
 permit Add a BGP Community List permit rule to specify extcommunity to
 accept

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

<DEVICE>(config-bgp-extcommunity-list-<EXTCOMMUNITY-LIST-NAME>)#
```

The following table summarizes the BGP extended community list configuration commands:

**Table 75: BGP-Ext-Community-List Config Mode Commands**

| Command                                                      | Description                                                                             |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| <a href="#">deny (bgp-ext-community-list)</a> on page 1867   | Creates and configures a deny extended community (expanded or standard) rule            |
| <a href="#">permit (bgp-ext-community-list)</a> on page 1868 | Creates and configures a permit extended community (expanded or standard) rule          |
| <a href="#">no (bgp-ext-community-list)</a> on page 1869     | Removes an existing deny or permit extended community rule from this ext community list |

### *deny (bgp-ext-community-list)*

Creates and configures a deny extended community (expanded or standard) rule

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

### Syntax

```
deny extcommunity [expanded|standard]
deny extcommunity expanded <LINE>
deny extcommunity standard [rt|soo] <COMMUNITY-NUMBER>
```

### Parameters

```
deny extcommunity expanded <LINE>
```

|                                                    |                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>deny extcommunity expanded &lt;LINE&gt;</pre> | <p>Configures a deny expanded named extended community list entry and associates it with a regular expression to match. The regular expression represents the patterns to match in the extended community attributes.</p> <ul style="list-style-type: none"><li>• &lt;LINE&gt; - Provide the regular expression.</li></ul> |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
deny extcommunity standard [rt|soo] <COMMUNITY-NUMBER>
```

|                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>deny extcommunity standard [rt  soo] &lt;COMMUNITY-NUMBER&gt;</pre> | <p>Configures a deny standard named extended community list entry, and associates it with the target or origin community attributes.</p> <ul style="list-style-type: none"><li>• rt - Configures the RT (route target) extended community attribute</li><li>• soo - Configures the SOO (site-of-origin) extended community attribute</li></ul> <p>&lt;COMMUNITY-NUMBER&gt; - Specify the community number in one of the following formats: AA:NN or A.B.C.D:NN</p> |
|--------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config-bgp-extcommunity-list-test)#deny extcommunity standard rt 200:12
nx9500-6C8809(config-bgp-extcommunity-list-test)#show context
bgp extcommunity-list test
 deny extcommunity standard rt 200:12
nx9500-6C8809(config-bgp-extcommunity-list-test)#
```

### Related Commands

|                                                     |                                                                                       |
|-----------------------------------------------------|---------------------------------------------------------------------------------------|
| <pre>no (bgp-ext-community-list) on page 1869</pre> | <p>Removes the specified deny extended community rule from this extcommunity list</p> |
|-----------------------------------------------------|---------------------------------------------------------------------------------------|

### *permit (bgp-ext-community-list)*

Creates and configures a permit extended community (expanded or standard) rule

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

### Syntax

```
permit extcommunity [expanded|standard]
permit extcommunity expanded <LINE>
permit extcommunity standard [rt|soo] <COMMUNITY-NUMBER>
```



## Parameters

```
permit extcommunity expanded <LINE>
```

|                                     |                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| permit extcommunity expanded <LINE> | Configures a permit expanded named extended community list entry and associates it with a regular expression to match. The regular expression represents the patterns to match in the extended community attributes. <ul style="list-style-type: none"><li>• &lt;LINE&gt; - Provide the regular expression.</li></ul> |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
permit extcommunity standard [rt|soo] <COMMUNITY-NUMBER>
```

|                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| permit extcommunity standard [rt soo] <COMMUNITY-NUMBER> | Configures a permit standard named extended community list entry, and associates it with the target or origin community attributes. <ul style="list-style-type: none"><li>• rt - Configures the RT extended community attribute</li><li>• soo - Configures the SOO extended community attribute</li></ul> <COMMUNITY-NUMBER> - Specify the community number in one of the following formats: AA:NN or A.B.C.D:NN |
|----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-bgp-extcommunity-list-test)#permit extcommunity standard rt 300:03
nx9500-6C8809(config-bgp-extcommunity-list-test)#show context
bgp extcommunity-list test
 permit extcommunity standard rt 300:03
 deny extcommunity standard rt 200:12
nx9500-6C8809(config-bgp-extcommunity-list-test)#
```

## Related Commands

|                                          |                                                                                  |
|------------------------------------------|----------------------------------------------------------------------------------|
| no (bgp-ext-community-list) on page 1869 | Removes the specified permit extended community rule from this extcommunity list |
|------------------------------------------|----------------------------------------------------------------------------------|

*no (bgp-ext-community-list)*

Removes an existing deny or permit extended community rule from this extcommunity list

## Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

## Syntax

```
no [deny|permit] extcommunity expanded <LINE>
no [deny|permit] extcommunity standard [rt|soo] <COMMUNITY-NUMBER>
```

## Parameters

```
no <PARAMETERS>
```

|                 |                                                                                    |
|-----------------|------------------------------------------------------------------------------------|
| no <PARAMETERS> | Removes a deny or permit expanded extended community rule from this community list |
|-----------------|------------------------------------------------------------------------------------|

## Examples

The following example shows the extended community 'test' settings before the 'no' command is executed:

```
nx9500-6C8809(config-bgp-extcommunity-list-test)#show context
bgp extcommunity-list test
 permit extcommunity standard rt 300:03
 deny extcommunity standard rt 200:12
nx9500-6C8809(config-bgp-extcommunity-list-test)#
nx9500-6C8809(config-bgp-extcommunity-list-test)#no permit extcommunity standard 300:03
```

The following example shows the extended community 'test' settings after the 'no' command is executed:

```
nx9500-6C8809(config-bgp-extcommunity-list-test)#show context
bgp extcommunity-list test
 deny extcommunity standard rt 200:12
nx9500-6C8809(config-bgp-extcommunity-list-test)#
```

## bgp route-map

BGP route maps are used to control and modify routing information. A BGP route map is a collection of deny and/or permit route rules that define and control redistribution of routes between routers and routing processes. Each rule consists of match criteria and set lines. If a route matches a criteria, the corresponding set line is applied, and the route is passed to the BGP table or to the neighbor, depending on whether the route map is set for incoming or outgoing route updates.

Use the (config) instance to configure BGP route map related parameters.

To navigate to this instance, use the following command:

```
<DEVICE>(config)#route-map <ROUTE-MAP-NAME>
<DEVICE>(config)#route-map test
<DEVICE>(config-dr-route-map-test)#?
Route Map Mode commands:
 deny Add a deny route map rule to deny set operations
 no Negate a command or set its defaults
 permit Add a permit route map rule to permit set operations

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

<DEVICE>(config-dr-route-map-test)#
```

In the route-map configuration mode, use the following commands to create and configure a deny or permit route map rule:

```
<DEVICE>(config-dr-route-map-test)#deny route-map <1-65535>
<DEVICE>(config-dr-route-map-test)#permit route-map <1-65535>
```

For example:

```
<DEVICE>(config-dr-route-map-test)#permit route-map 1
<DEVICE>(config-dr-route-map-test)#deny route-map 2
<DEVICE>(config-dr-route-map-test)#show context
route-map test
 permit route-map 1
 deny route-map 2
<DEVICE>(config-dr-route-map-test)#
<DEVICE>(config-dr-route-map-test-dr-route-map-rule-1)#?
Route Map Rule Mode commands:
 description Configure comment for this route map
 match Match values from routing table
 no Negate a command or set its defaults
 set Set values in destination routing protocol

 clrscr Clears the display screen
 commit Commit all changes made in this session
 do Run commands from Exec mode
 end End current mode and change to EXEC mode
 exit End current mode and down to previous mode
 help Description of the interactive help system
 revert Revert changes
 service Service Commands
 show Show running system information
 write Write running configuration to memory or terminal

<DEVICE>(config-dr-route-map-test-dr-route-map-rule-1)#
```

The following table summarizes BGP Route Map deny/permit route map rules configuration mode commands:

**Table 76: BGP-Route-Map Config Mode Commands**

| Command                                                  | Description                                                                                                                                  |
|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">description (bgp-route-map)</a> on page 1871 | Configures a description for this route-map rule (deny or permit) that uniquely distinguishes it from others with similar access permissions |
| <a href="#">match (bgp-route-map)</a> on page 1872       | Configures the match criteria associated with this deny or permit BGP route map                                                              |
| <a href="#">set (bgp-route-map)</a> on page 1875         | Configures the values attributed to a route matching the match criteria specified in the BGP deny or permit route-map rules                  |
| <a href="#">no (bgp-route-map)</a> on page 1878          | Removes or reverts the settings defined for a deny or permit route-map rule                                                                  |

*description (bgp-route-map)*

Configures a description for this route map rule (deny or permit) that uniquely distinguishes it from others with similar access permissions

**Supported in the following platforms:**

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

## Syntax

```
description <LINE>
```

## Parameters

```
description <LINE>
```

|                    |                                                                                          |
|--------------------|------------------------------------------------------------------------------------------|
| description <LINE> | Provide a description for the route map rule (should not exceed 64 characters in length) |
|--------------------|------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#description "This is
a deny route map rule"
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#show context
deny route-map 1
 description "This is a deny route map rule"
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#
```

## Related Commands

|                                              |                                                       |
|----------------------------------------------|-------------------------------------------------------|
| <code>no (bgp-route-map)</code> on page 1878 | Removes this deny/permit route-map rule's description |
|----------------------------------------------|-------------------------------------------------------|

## *match (bgp-route-map)*

Configures the match criteria associated with this deny or permit BGP route map

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

## Syntax

```
match [as-path|community|extcommunity|ip-address|ip-next-hop|ip-route-source|metric|origin|
tag]
match [as-path <AS-PATH-LIST-NAME>|community <COMMUNITY-LIST-NAME> {exact-match}|
extcommunity <EXTCOMMUNITY-LIST-NAME>]
match [ip-address|ip-next-hop|ip-route-source] [BGP-IP-ACCESS-LIST <BGP-ACL-NAME>|prefix-
list <PREFIX-LIST-NAME>]
match metric <0-4294967295>
match origin [egp|igp|incomplete]
match tag <0-65535>
```

## Parameters

```
match [as-path <AS-PATH-LIST-NAME>|community <COMMUNITY-LIST-NAME> {exact-match}|
extcommunity <EXTCOMMUNITY-LIST-NAME>]
```

|                                               |                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| as-path <AS-PATH-LIST-NAME>                   | Configures a BGP AS path list to match<br>An AS path is a list of ASs a packet traverses to reach its destination. <ul style="list-style-type: none"> <li>&lt;AS-PATH-LIST-NAME&gt; - Specify the AS path list name (should be existing and configured)</li> </ul>                                                                                 |
| community <COMMUNITY-LIST-NAME> {exact-match} | Configures the AS community list string to match <ul style="list-style-type: none"> <li>&lt;COMMUNITY-LIST-NAME&gt; - Specify the AS community list name (should be existing and configured).</li> <li>exact-match - Optional. Does an exact match when matching the specified AS community string. This option is disabled by default.</li> </ul> |
| extcommunity <EXTCOMMUNITY-LIST-NAME>         | Configures the external community list string to match <ul style="list-style-type: none"> <li>&lt;EXTCOMMUNITY-LIST-NAME&gt; - Specify the external community list name (should be existing and configured).</li> </ul>                                                                                                                            |

```
match [ip-address|ip-next-hop|ip-route-source] [BGP-IP-ACCESS-LIST <BGP-ACL-NAME>|
prefix-list <PREFIX-LIST-NAME>]
```

|                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| match                                                                               | Configures match criteria used to filter BGP routes when forwarding packets                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| ip-address [BGP-IP-ACCESS-LIST <BGP-ACL-NAME>] prefix-list <PREFIX-LIST-NAME>]      | Configures a string of IP addresses, in the route, to match<br>The IP Address is a list of IP addresses in the route used to filter the route. Use one of the following options to provide a list of IP addresses: <ul style="list-style-type: none"> <li>BGP-IP-ACCESS-LIST &lt;BGP-ACL-NAME&gt; - Associates an existing BGP ACL with this BGP route map. Specify the BGP ACL name (should be existing and configured).</li> <li>prefix-list &lt;PREFIX-LIST-NAME&gt; - Associates an existing IP address prefix list with this BGP route map. The IP Address Prefix List is a list of prefixes in the route used to filter route. Specify the prefix list name (should be existing and configured).</li> </ul>                                                                                    |
| ip-next-hop [BGP-IP-ACCESS-LIST <BGP-ACL-NAME>] prefix-list <PREFIX-LIST-NAME>]     | Configures the next-hop's IP address to match<br>The IP Next Hop is a list of IP addresses used to filter routes based on the IP address of the next-hop in the route. Use one of the following options to provide next-hop's IP addresses: <ul style="list-style-type: none"> <li>BGP-IP-ACCESS-LIST &lt;BGP-ACL-NAME&gt; - Associates an existing BGP ACL with this BGP route map. Specify the BGP ACL name (should be existing and configured).</li> <li>prefix-list &lt;PREFIX-LIST-NAME&gt; - Associates an existing IP next-hop prefix list with this BGP route map. The IP Next Hop Prefix List is a list of prefixes for the route's next-hop determining how the route is filtered. Specify the prefix list name (should be existing and configured).</li> </ul>                            |
| ip-route-source [BGP-IP-ACCESS-LIST <BGP-ACL-NAME>] prefix-list <PREFIX-LIST-NAME>] | Configures the advertised route source IP address to match<br>The IP Route Source is a list of IP addresses used to filter routes based on the advertised IP address of the source. Use one of the following options to provide route-source IP addresses: <ul style="list-style-type: none"> <li>BGP-IP-ACCESS-LIST &lt;BGP-ACL-NAME&gt; - Associates an existing BGP ACL with this BGP route map. Specify the BGP ACL name (should be existing and configured).</li> <li>prefix-list &lt;PREFIX-LIST-NAME&gt; - Associates an existing IP route source prefix list with this BGP route map. The IP Route Source Prefix List is a list of prefixes used to filter routes based on the prefix list used for the source. Specify the prefix list name (should be existing and configured).</li> </ul> |

```
match metric <0-4294967295>
```

```
match metric <0-4294967295>
```

Defines the exterior metric, used for route map distribution, to match BGP uses a route table managed by the external metric defined. Setting a metric provides a dynamic way to load balance between routes of equal cost.

- <0-4294967295> – Specify the external metric value from 0 - 4294967295.

```
match origin [egp|igp|incomplete]
```

```
match origin [egp|igp|incomplete]
```

Configures the source of the BGP route to match. Options include:

- **egp** – Matches if the origin of the route is from the eBGP. eBGP exchanges routing table information between hosts outside an autonomous system.
- **igp** – Matches if the origin of the route is from the iBGP. iBGP exchanges routing table information between routers within an autonomous system.
- **incomplete** – Matches if the origin of the route is not identifiable

```
match tag <0-65535>
```

```
match tag <0-65535>
```

Configures the BGP route tag to match

The Tag is a way to preserve a route's AS path information for routers in iBGP. This option is disabled by default.

- <0-65535> – Specify the iBGP route's tag from 0 - 65535.

## Examples

The following examples show the configuration of match criteria for the deny route-map rule 1:

```
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#match as-path FilterList_01
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#match ip-route-source prefix-list PrefixList_01
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#show context
deny route-map 1
 description "This is a deny route map rule"
 match as-path FilterList_01
 match ip-route-source prefix-list PrefixList_01
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#
```

A permit route-map rule 2 is added to the BGP route-map "test".

```
nx9500-6C8809(config-dr-route-map-test)#permit route-map 2
```

A match criteria is added for the permit route-map rule 2.

```
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-2)#match ip-next-hop DL_01
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-2)#show context
permit route-map 2
 match ip-next-hop DL_01
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-2)#
```

The following example displays the BGP route-map "test" settings:

```
nx9500-6C8809(config-dr-route-map-test)#show context
route-map test
 deny route-map 1
 description "This is a deny route map rule"
 match as-path FilterList_01
 match ip-route-source prefix-list PrefixList_01
 permit route-map 2
```

```
match ip-next-hop DL_01
nx9500-6C8809(config-dr-route-map-test)#
```

## Related Commands

`no (bgp-route-map)` on page 1878 Removes match criteria associated with a deny or permit route-map rule

## *set (bgp-route-map)*

Configures the values attributed to a route matching the match criteria specified in the BGP deny or permit route-map rules. These attributes are applied before the route is sent out.

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

### Syntax

```
set [aggregator-as|as-path|atomic-aggregate|comm-list|community|extcommunity|ip|
local-preference|metric|origin|originator-id|source-ip|tag|weight]
set aggregator-as <1-4294967295> <IP>
set as-path [exclude|prepend] <1-4294967295> {<1-4294967295>}
set atomic-aggregate
set comm-list delete <COMMUNITY-LIST-NAME>
set community [<COMMUNITY-NUMBER>|none]
set extcommunity [rt|soo] <EXTCOMMUNITY-NUMBER>
set ip next-hop [<IP>|peer-address]
set local-preference <0-4294967295>
set metric <0-4294967295>
set origin [egp|igp|incomplete]
set originatorid <IP>
set source-ip <IP>
set tag <0-65535>
set weight <0-4294967295>
```

### Parameters

```
set aggregator-as <1-4294967295> <IP>
```

|                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>set aggregator-as &lt;1-4294967295&gt; &lt;IP&gt;</pre> | <p>Configures the BGP aggregator's ASN and IP address. Aggregates minimize the size of routing tables. Aggregation combines the characteristics of multiple routes and advertises them as a single route. The configured BGP aggregator settings are applied to filtered routes.</p> <ul style="list-style-type: none"><li>• &lt;1-4294967295&gt; - Specify the route aggregator's ASN from 1-4294967295. This option is disabled by default.</li><li>• &lt;IP&gt; - Specify the route aggregator's IP address. BGP allows the aggregation of specific routes into one route using an aggregate IP address.</li></ul> |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
set as-path [exclude|prepend] <1-4294967295> {<1-4294967295>}
```

|                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>set as-path [exclude prepend] &lt;1-4294967295&gt; {&lt;1-4294967295&gt;}</pre> | <p>Configures the BGP transform AS path attribute to be applied to filtered routes</p> <ul style="list-style-type: none"> <li>• exclude – Configures a single AS, or a list of ASs, excluded from the AS path</li> <li>• prepend – Configures a single AS, or a list of ASs, prepended to the AS path <ul style="list-style-type: none"> <li>• &lt;1-4294967295&gt; – This keyword is common to the ‘exclude’ and ‘prepend’ parameters. Use it to specify the AS number. The ASs identified here are excluded or prepended depending on the option selected.</li> </ul> </li> </ul> <p>You can configure multiple ASNs.</p> |
|--------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

`set atomic-aggregate`

|                                 |                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>set atomic-aggregate</pre> | <p>Enables BGP atomic aggregate attributes</p> <p>When a BGP enabled wireless controller or service platform receives a set of overlapping routes from a peer, or if the set of routes selects a less specific route, then the local device must set this value when propagating the route to its neighbors. This option is disabled by default.</p> |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

`set comm-list delete <COMMUNITY-LIST-NAME>`

|                                                              |                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>set comm-list delete &lt;COMMUNITY- LIST-NAME&gt;</pre> | <p>Deletes specified BGP communities. All communities matching the community list name string are deleted from the route.</p> <p>A BGP community is a group of routes sharing a common attribute.</p> <ul style="list-style-type: none"> <li>• &lt;COMMUNITY-LIST-NAME&gt; – Specify the community list name.</li> </ul> |
|--------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

`set community [<COMMUNITY-NUMBER>|none]`

|                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>set community [&lt;COMMUNITY- NUMBER&gt; none]</pre> | <p>Configures a community attribute for this route</p> <ul style="list-style-type: none"> <li>• &lt;COMMUNITY-NUMBER&gt; – Specify a community attribute. Use one of the following formats: <ul style="list-style-type: none"> <li>• internet - Advertises this route to the Internet. This is a global community.</li> <li>• local-AS - Prevents the transmit of packets outside the local AS</li> <li>• no-advertise - Prevents advertisement of this route to any peer, either internal or external</li> <li>• no-export - Prevents advertisement of this route to BGP peers, keeping this route within an AS.</li> <li>• aa:nn - Configures the first part (aa) representing the AS number. The second part (nn) represents a 2-byte number.</li> </ul> </li> <li>• none – Specifies community attribute as none</li> </ul> |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

`set extcommunity [rt|soo] <EXTCOMMUNITY-NUMBER>`



|                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>set extcommunity [rt soo] &lt;EXTCOMMUNITY-NUMBER&gt;</pre> | <p>Configures a extended community attribute for this route</p> <ul style="list-style-type: none"> <li>• rt - Identifies the route target (rt) extended community</li> <li>• soo - Identifies the site-of-origin (soo) community. This is the origin community associated with the route reflector.</li> <li>• &lt;EXTCOMMUNITY-NUMBER&gt; - This keyword is common to the 'rt' and 'soo' parameters. Use it to specify the extended community number.</li> </ul> |
|------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
set ip next-hop [<IP>|peer-address]
```

|                                                      |                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>set ip next-hop [&lt;IP&gt; peer-address]</pre> | <p>Configures the next hop for this route. Use one of the following options to identify the next hop:</p> <ul style="list-style-type: none"> <li>• &lt;IP&gt; - Specify the nest hop's IP address</li> <li>• peer-address - Enables the identification of the next-hop address for peer devices. This option is disabled by default</li> </ul> |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
set local-preference <0-4294967295>
```

|                                                      |                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>set local-preference &lt;0-4294967295&gt;</pre> | <p>Configures the BGP local preference path attribute for this route map. When configured, enables the communication of preferred routes out of the AS between peers. This option is disabled by default.</p> <ul style="list-style-type: none"> <li>• &lt;0-4294967295&gt; - Specify the preference value from 0 - 4294967295.</li> </ul> |
|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
set metric <0-4294967295>
```

|                                            |                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>set metric &lt;0-4294967295&gt;</pre> | <p>Configures a metric for the route BGP uses a route table managed by the external metric defined. Setting a metric provides a dynamic way to load balance between routes of equal cost.</p> <ul style="list-style-type: none"> <li>• &lt;0-4294967295&gt; - Specify the metric from 0 - 4294967295.</li> </ul> |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
set origin [egp|igp|incomplete]
```

|                                            |                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>set origin [egp igp incomplete]</pre> | <p>Configures the origin code for this BGP route map</p> <ul style="list-style-type: none"> <li>• egp - Sets the origin of the route to eBGP</li> <li>• igp - Sets the origin of the route to iBGP</li> <li>• incomplete - Sets the origin of the route as not identifiable. Use this option if the route is from a source other than eBGP or iBGP.</li> </ul> |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
set originatorid <IP>
```

|                                        |                                                          |
|----------------------------------------|----------------------------------------------------------|
| <pre>set originatorid &lt;IP&gt;</pre> | <p>Configures this route map's originator IP address</p> |
|----------------------------------------|----------------------------------------------------------|

```
set source-ip <IP>
```

|                                     |                                                                                                                                                                     |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>set source-ip &lt;IP&gt;</pre> | <p>Configures this route map's source IP address</p> <ul style="list-style-type: none"> <li>• &lt;IP&gt; - Specify the IP address in the A.B.C.D format.</li> </ul> |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
set tag <0-65535>
```

```
set tag <0-65535>
```

Configures this route map's tag value  
The Tag is a way to preserve a route's AS path information for routers in iBGP.

- <0-65535> - Specify a tag value from 0 - 65535.

```
set weight <0-4294967295>
```

```
set weight <0-4294967295>
```

Enables assignment of a weighted priority to the aggregate route

- <0-4292967295> - Specify a value from 0 - 4294967295.

## Examples

```
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#set aggregator-as 1
192.168.13.7
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#set as-path exclude 20
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#set community internet
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#set ip next-hop peer-address
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#set local-preference 30
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#set metric 300
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#show context
deny route-map 1
 description "This is a deny route map rule"
 match as-path FilterList_01
 match ip-route-source prefix-list PrefixList_01
 set aggregator-as 1 192.168.13.7
 set as-path exclude 20
 set ip next-hop peer-address
 set metric 300
 set local-preference 30
 set community internet
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#
```

## Related Commands

```
no (bgp-route-map) on page
1878
```

Removes the attributes configured for this route map

*no (bgp-route-map)*

Removes or reverts the settings defined for a deny or permit route-map rule

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

### Syntax

```
no [description|match <PARAMETERS>|set <PARAMETERS>]
```

### Parameters

```
no <PARAMETERS>
```

```
no <PARAMETERS>
```

Removes the description configured for a deny or permit route-map rule

## Examples

The following example shows the 'deny route-map rule-1' settings before the 'no' commands are executed:

```
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#show context
deny route-map 1
 description "This is a deny route map rule"
 match as-path FilterList_01
 match ip-route-source prefix-list PrefixList_01
 set aggregator-as 1 192.168.13.7
 set as-path exclude 20
 set ip next-hop peer-address
 set metric 300
 set local-preference 30
 set community internet
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#no match as-path
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#no set aggregator-as
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#no set metric
```

The following example shows the 'deny route-map rule-1' settings after the 'no' commands are executed:

```
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#show context
deny route-map 1
 description "This is a deny route map rule"
 match ip-route-source prefix-list PrefixList_01
 set as-path exclude 20
 set ip next-hop peer-address
 set local-preference 30
 set community internet
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#
```

The following example shows the route-map 'test' settings:

```
nx9500-6C8809(config-dr-route-map-test)#show context
route-map test
 deny route-map 1
 description "This is a deny route map rule"
 match ip-route-source prefix-list PrefixList_01
 set as-path exclude 20
 set ip next-hop peer-address
 set local-preference 30
 set community internet
 permit route-map 2
 match ip-next-hop DL_01
nx9500-6C8809(config-dr-route-map-test)#
```

## bgp router-config

Use the (device-config) or (profile-config) instance to configure BGP router related parameters.

To navigate to the BGP router configuration instance, in the device-config mode, use the following commands:

```
<DEVICE>(config)#self
<DEVICE>(config-device-<MAC>)#router bgp
<DEVICE>config-device <MAC>-router-bgp)#
<DEVICE>config-device <MAC>-router-bgp)#?
Router BGP Mode commands:
 aggregate-address Configure aggregate address
 asn Configure local Autonomous System Number
 bgp Border Gateway Protocol
```

|                     |                                                        |
|---------------------|--------------------------------------------------------|
| bgp-route-limit     | Limit for number of routes handled by BGP process      |
| distance            | Configure administrative distance                      |
| ip                  | Internet Protocol (IP)                                 |
| network             | Configure a local network                              |
| no                  | Negate a command or set its defaults                   |
| route- redistribute | Redistribute information from another routing protocol |
| timers              | Adjust routing timers                                  |
|                     |                                                        |
| clrscr              | Clears the display screen                              |
| commit              | Commit all changes made in this session                |
| do                  | Run commands from Exec mode                            |
| end                 | End current mode and change to EXEC mode               |
| exit                | End current mode and down to previous mode             |
| help                | Description of the interactive help system             |
| revert              | Revert changes                                         |
| service             | Service Commands                                       |
| show                | Show running system information                        |
| write               | Write running configuration to memory or terminal      |

```
<DEVICE>config-device <MAC>-router-bgp)#
```

When configured as a profile, the router settings are applied to all devices using the profile.

To navigate to the BGP router configuration instance, in the profile-config mode, use the following commands:

```
<DEVICE>(config)#profile <DEVICE-TYPE> <PROFILE-NAME>
<DEVICE>(config-profile-<PROFILE-NAME>)#router bgp
<DEVICE>(config-profile <PROFILE-NAME>-router-bgp)#
<DEVICE>(config-profile <PROFILE-NAME>-router-bgp)#?
```

Router BGP Mode commands:

|                     |                                                        |
|---------------------|--------------------------------------------------------|
| aggregate-address   | Configure aggregate address                            |
| asn                 | Configure local Autonomous System Number               |
| bgp                 | Border Gateway Protocol                                |
| bgp-route-limit     | Limit for number of routes handled by BGP process      |
| distance            | Configure administrative distance                      |
| ip                  | Internet Protocol (IP)                                 |
| network             | Configure a local network                              |
| no                  | Negate a command or set its defaults                   |
| route- redistribute | Redistribute information from another routing protocol |
| timers              | Adjust routing timers                                  |
|                     |                                                        |
| clrscr              | Clears the display screen                              |
| commit              | Commit all changes made in this session                |
| do                  | Run commands from Exec mode                            |
| end                 | End current mode and change to EXEC mode               |
| exit                | End current mode and down to previous mode             |
| help                | Description of the interactive help system             |
| revert              | Revert changes                                         |
| service             | Service Commands                                       |
| show                | Show running system information                        |
| write               | Write running configuration to memory or terminal      |

```
<DEVICE>(config-profile <PROFILE-NAME>-router-bgp)#
```

The following table summarizes BGP router configuration mode commands:

**Table 77: BGP-Router Config Mode Commands**

| Command                                                             | Description                                                                   |
|---------------------------------------------------------------------|-------------------------------------------------------------------------------|
| <a href="#">aggregate (bgp-router-config)</a> on page 1881          | Creates and configures an aggregate address entry in the BGP database         |
| <a href="#">asn (bgp-router-config)</a> on page 1882                | Configures this BGP router's ASN                                              |
| <a href="#">bgp (bgp-router-config)</a> on page 1882                | Configures BGP router parameters                                              |
| <a href="#">bgp-route-limit (bgp-router-config)</a> on page 1887    | Configures the BGP route limit parameters                                     |
| <a href="#">distance (bgp-router-config)</a> on page 1888           | Configures administrative distance parameters                                 |
| <a href="#">ip (bgp-router-config)</a> on page 1889                 | Configures the BGP default gateway's priority                                 |
| <a href="#">network (bgp-router-config)</a> on page 1890            | Configures the local network IP addresses and masks                           |
| <a href="#">route-redistribute (bgp-router-config)</a> on page 1891 | Enables redistribution of routes learnt from other routing protocols into BGP |
| <a href="#">timers (bgp-router-config)</a> on page 1892             | Enables adjustment of keepalive and holdtime intervals                        |
| <a href="#">no (bgp-router-config)</a> on page 1893                 | Removes the BGP router settings                                               |

### *aggregate (bgp-router-config)*

Creates and configures an aggregate address entry in the BGP database

#### **Supported in the following platforms:**

- Wireless Controllers – RFS 4000
- Service Platforms – NX 95XX, NX 96XX

#### **Syntax**

```
aggregate-address <IP/M> {as-set {summary-only}|summary-only}
```

#### **Parameters**

```
aggregate-address <IP/M> {as-set {summary-only}|summary-only}
```

|                          |                                                                                                                                                                                                        |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| aggregate-address <IP/M> | Specify the aggregate IP address and mask                                                                                                                                                              |
| as-set {summary-only}    | Optional. Summarizes the AS_PATH attributes of the individual routes aggregated <ul style="list-style-type: none"> <li>• summary-only – Optional. Filters more specific routes from updates</li> </ul> |

#### **Examples**

```

nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#aggregate-address
192.168.13.10/32 as-set summary-only
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#show context
router bgp
 bgp enable
 asn 1
 aggregate-address 192.168.13.10/32 as-set summary-only

```

```

 bgp neighbor 192.168.13.199
 remote-as 1
 use route-map UnSupMap_01 in
 bgp neighbor 192.168.13.99
 remote-as 199
 timers connect 10
 timers 20 40
 maximum-prefix 9999 80 restart 50
 bgp neighbor 1.1.1.1
 remote-as 2
 timers connect 10
 timers 20 40
 maximum-prefix 1000000
 bgp-route-limit num-routes 10 reset-time 360
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#

```

### Related Commands

|                                                  |                                     |
|--------------------------------------------------|-------------------------------------|
| <code>no (bgp-router-config)</code> on page 1893 | Removes the aggregate address entry |
|--------------------------------------------------|-------------------------------------|

### *asn (bgp-router-config)*

Configures the ASN. The ASN represents a group of routers under the same administration and using IGP and common metrics to define how to route packets. In short the ASN represents all routers within an AS.

#### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

#### Syntax

```
asn <1-4294967295>
```

#### Parameters

```
asn <1-4294967295>
```

|                                       |                                      |
|---------------------------------------|--------------------------------------|
| <code>asn &lt;1-4294967295&gt;</code> | Specify the ASN from 1 - 4294967295. |
|---------------------------------------|--------------------------------------|

#### Examples

```

nx9500-6C8809(config-profile NX9500Profile-router-bgp)#asn 1
nx9500-6C8809(config-profile NX9500Profile-router-bgp)#show context
 router bgp
 asn 1
nx9500-6C8809(config-profile NX9500Profile-router-bgp)#

```

#### Related Commands

|                                                  |                                 |
|--------------------------------------------------|---------------------------------|
| <code>no (bgp-router-config)</code> on page 1893 | Removes the configured the ASN. |
|--------------------------------------------------|---------------------------------|

### *bgp (bgp-router-config)*

Configures BGP router parameters

## Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

## Syntax

```
bgp [always-compare-med|bestpath|client-to-client|cluster-id|confederation|
dampening|default|deterministic-med|enable|enforce-first-as|fast-external-failover|
graceful-restart|log-neighbor-changes|neighbor|network|router-id|scan-time]
bgp [always-compare-med|deterministic-med|enable|enforce-first-as|
fast-external-failover|log-neighbor-changes]
bgp best-path [as-path [confed|ignore]|compare-router-id|med {confed {missing-as-worst}}|
missing-as-worst}]
bgp client-to-client reflection
bgp cluster <IP>
bgp confederation [identifier|peers] <1-4294967295>
bgp dampening {<1-45>} {<1-20000>} <1-20000> <1-255>
bgp default [ipv4-unicast|local-preference <0-4294967295>]
bgp graceful-restart {stalepath-time <1-3600>}
bgp neighbor <IP>
bgp network import-check
bgp router-id <IP>
bgp scan-time <5-60>
```

## Parameters

```
bgp [always-compare-med|deterministic-med|enable|enforce-first-as|
fast-external-failover|log-neighbor-changes]
```

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| always-compare-med | Enables comparison of MEDs (Multi-exit Discriminators) received from neighbors. This option is disabled by default.<br>MED is a value used by BGP peers to select the best route among multiple routes. When enabled, the MED value encoded in the route is always compared when selecting the best route to the host network. A route with a lower MED value is preferred over a route with a higher MED value. BGP does not discriminate between iBGP and eBGP when using MED for route selection. This option is mutually exclusive to the <i>deterministic-med</i> option. |
| deterministic-med  | Enables selection of the best MED path from amongst all paths advertised by neighboring ASs. This option is disabled by default.<br>MED is used by BGP peers to select the best route among multiple routes. When enabled, MED route values (from the same AS) are compared to select the best route. This best route is then compared with other routes in the BGP route table to select the best overall route. This option is mutually exclusive to the always-compare-med option.                                                                                          |
| enable             | Starts the BGP daemon on the device (wireless controller or service platform). BGP is disabled by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| enforce-first-as   | Enforces the first AS for all BGP routes. This option is disabled by default. When enforced, devices deny updates received from an external neighbor that does not have the neighbor's configured AS at the beginning of the received AS path parameter. This enhances security by not allowing traffic from an unauthorized AS.                                                                                                                                                                                                                                               |

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| fast-external-failover | <p>Enables immediate resetting of BGP session on the interface once the BGP connection goes down. This option is enabled by default.</p> <p>When enabled, a session is reset as soon as the direct link to an external peer goes down. Normally, when a BGP connection goes down, the device waits for the expiry of the duration specified in holdtime parameter before bringing down the interface.</p> <p>To configure the 'holdtime', use the <b>timers &gt; bgp &gt; &lt;keepalive-time&gt; &gt; &lt;holdtime&gt;</b> command in this (BGP router) configuration mode.</p> |
| log-neighbor-changes   | <p>Enables logging of a BGP neighbor's status change (active or not active) events. It also enables the logging of the reason for such change in status.</p>                                                                                                                                                                                                                                                                                                                                                                                                                    |

```
bgp best-path [as-path [confed|ignore]|compare-router-id|med {confed {missing-as-worst}}|missing-as-worst}]
```

|                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| best-path                                         | <p>Modifies the bestpath selection algorithm. The route selection algorithm uses the following criteria when selecting the preferred route: as-path, router-id, and med.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| as-path [confed ignore]                           | <p>Enables an AS path from being considered as a criteria for selecting the preferred route</p> <ul style="list-style-type: none"> <li>• confed – Enables comparison of path lengths (including confederation sets and sequences) when selecting a route (EXPERIMENTAL). This option is disabled by default.</li> <li>• ignores – Disables an AS path length from being considered as a criteria for selecting a preferred route. When, disabled the AS path length is ignored. This option is disabled by default.</li> </ul>                                                                                                                                                                                                                                                                                                                                  |
| compare-router-id                                 | <p>Enables the use of router ID as a selection criteria when selecting the preferred route. When enabled, the router ID is used to select the best path between two identical BGP routes. The route with the lower router ID is selected over a route with a higher router ID. This option is disabled by default.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| med {confed {missing-as-worst}} missing-as-worst} | <p>Enables comparison of AS path MED value when selecting the preferred route</p> <p>MED is a value used by BGP peers to select the best route among multiple routes. When enabled, the MED value encoded in the route is always compared to determine the best route to the host network. A route with a lower MED value is preferred over a route with a higher MED value.</p> <ul style="list-style-type: none"> <li>• confed – Optional. Enables comparison of MED value among confederation paths (EXPERIMENTAL). When enabled, you can optionally enable the treatment of AS paths without the MED value as the least preferable route. This option is disabled by default.</li> <li>• missing-as-worst – Optional. Enables the treatment of AS paths without the MED value as the least preferable route. This option is disabled by default.</li> </ul> |

```
bgp client-to-client reflection
```

|                             |                                                                                                                                                                                                                                                          |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| client-to-client reflection | <p>Enables client-to-client route reflection (EXPERIMENTAL)</p> <p>Route reflectors are used when all iBGP speakers are not fully meshed. If the clients are fully meshed, the route-reflectors are not required. This option is enabled by default.</p> |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
bgp cluster <IP>
```



cluster <IP>

Enables and sets a cluster ID, in case the BGP cluster has more than one route-reflector  
A cluster generally consists of a single route-reflector and its clients. The cluster is usually identified by the router ID of this single route-reflector. Sometimes, to increase redundancy, a cluster might have more than one route-reflector configured. In this case, all route-reflectors in the cluster are identified by the cluster ID (configured in the IP format).

`bgp confederation [identifier|peers] <1-4294967295>`

confederation [identifier|peers]  
<1-4294967295>

Configures AS confederation (group of ASs) parameters (identifier and peers)

- identifier – Enables and sets a BGP confederation identifier to allow an AS to be divided into several ASs. In other words an AS is divided into multiple ASs, and together they form a confederation. This confederation is visible to external routers as a single AS. The ASN is usually the confederation ID. Specify a value from 1 - 4294967295.

Forming AS confederation reduces iBGP mesh inside an AS.

- peers – Configures the maximum number of the ASs constituting this BGP confederation. Specify the AS number from 1 - 4294967295. Multiple ASs can be added to the list of confederation members.

`bgp dampening {<1-45>} {<1-20000>} <1-20000> <1-255>`

bgp dampening {<1-45>}  
{<1-20000>} <1-20000> <1-255>

Enables dampening and configures dampening parameters. This option is disabled by default.  
Dampening minimizes the instability caused by route flapping. A penalty is added for every flap in the flapping route. As soon as the total penalty reaches the specified Route Suppress Limit value, the advertisement of this route is suppressed. This penalty is delayed when the time specified in Half Lifetime occurs. Once the penalty becomes lower than the value specified in Start Route Reuse, the advertisement of the route is un-suppressed.

- <1-45> – Optional. Configures the half lifetime (in minutes). A penalty is imposed on a route that flaps. This is the time for the penalty to decrease to half its current value. Specify a value from 1 - 45 minutes. The default is 1 minute.
- <1-20000> – Optional. Configures the route reuse value. When the penalty for a suppressed route decays below the value specified here, the route is un-suppressed (reused). Specify a value from 1 - 20000.
- <1-20000> – Configures the route suppress value. When a route flaps, a penalty is added to the route. When the penalty reaches or exceeds the value specified as the 'maximum duration to suppress a stable route'. Specify a value from 1 - 20000.

The maximum duration to suppress a stable route, is the next set of value configured in this command from 1 - 255.

- <1-255> – Configures the maximum duration, in minutes, a suppressed route is suppressed. This is the maximum duration for which a route remains suppressed before it is reused. Specify a value from 1 - 255 minutes.

`bgp default [ipv4-unicast|local-preference <0-4294967295>]`

|                                 |                                                                                                                                                                                                           |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| default                         | Configures the following defaults for BGP neighbor-related parameters: IPv4 unicast and local preference                                                                                                  |
| ipv4-unicast                    | Enable IPv4 unicast traffic for neighbors. This option is enabled by default.                                                                                                                             |
| local-preference <0-4294967295> | Configures a local preference for the neighbor. Higher the value higher is the preference. <ul style="list-style-type: none"> <li>&lt;0-4294967295&gt; – Specify a value from 10 - 4294967295.</li> </ul> |

`bgp graceful-restart {stalepath-time <1-3600>}`

|                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| default graceful-restart {stalepath-time <1-3600>} | Enables graceful restart on this BGP router. This option is disabled by default <ul style="list-style-type: none"> <li>stalepath-time &lt;1-3600&gt; – Optional. Configures the maximum time, in seconds, to retain stale paths from restarting neighbor. This is the time the paths from a restarting neighbor are preserved. All stale paths, unless reinstated by the neighbor after re-establishment, are deleted at the expiry of the time specified here. <ul style="list-style-type: none"> <li>&lt;1-3600&gt; – Specify a value from 1 - 3600 seconds.</li> </ul> </li> </ul> |
|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

`bgp neighbor <IP>`

|               |                                                                                                                                                                                                                                                                                                                                                      |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| neighbor <IP> | Configures the BGP neighbor's IP address and enters its configuration mode. Use this command to configure a BGP neighbor's parameters. <ul style="list-style-type: none"> <li>&lt;IP&gt; – Specify the IP address in the A.B.C.D format.</li> </ul> <p>For BGP neighbor configuration parameters, see <code>bgp-neighbor-config</code> commands.</p> |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

`bgp network import-check`

|                      |                                                                                |
|----------------------|--------------------------------------------------------------------------------|
| network import-check | Enables checking of the existence of BGP network route in IGP before importing |
|----------------------|--------------------------------------------------------------------------------|

`bgp router-id <IP>`

|             |                                                                                                                                                                                                                                                                                                                               |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| router <IP> | Enables the device (BGP supported wireless controller or service platform) identified by the <IP> parameter as a router. The router's IP address is configured as its ID, and uniquely identifies it. When not specified, the IP address of the interface is configured as the router ID. This option is disabled by default. |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

`bgp scan-time <5-60>`

scan-time <5-60>

Configures the scanning interval, in seconds, for updating BGP routes. This is the interval between two consecutive scans the BGP device performs in order to validate routes in its routing table. To disable scanning, set the value to Zero (0).

- <5-60> - Specify a value from 5 - 60 seconds. The default is 60 seconds.

## Examples

```
nx9500-6C8809(config-profile testNX9000-router-bgp)#bgp router-id 192.168.13.13
nx9500-6C8809(config-profile testNX9000-router-bgp)#aggregate-address 116.117.118.0/24 as-
set summary-only
nx9500-6C8809(config-profile testNX9000-router-bgp)#bgp neighbor 192.168.13.99
nx9500-6C8809(config-profile testNX9000-router-bgp)#show context
router bgp
 aggregate-address 116.117.118.0/24 as-set summary-only
 bgp router-id 192.168.13.13
 bgp neighbor 192.168.13.99
 remote-as 199
 maximum-prefix 9999 80 restart 50
nx9500-6C8809(config-profile testNX9000-router-bgp)#
```

## Related Commands

**no (bgp-router-config)** on  
page 1893

Removes the BGP router parameters. The no > bgp > enable command disabled BGP.

## *bgp-route-limit (bgp-router-config)*

Configures the BGP route limit parameters

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

### Syntax

```
bgp-route-limit [num-routes <VALUE>|reset-time <1-86400>|retry-count <1-32>|
retry-timeout <1-3600>]
```

### Parameters

```
bgp-route-limit [num-routes <VALUE>|reset-time <1-86400>|retry-count <1-32>|
retry-timeout <1-3600>]
```

num-routes <VALUE>

Configures the number of routes that can be stored on this BGP router. Set this value based on the available memory on this BGP router (wireless controller or service platform).

- <VALUE> - Specify a value from 1 - 4,294,967,295. The default is 9216 routes.

reset-time <1-86400>

Configures the reset time in seconds. This is the time after which the retry count value is set to Zero (0).

- <1-86400> - Specify a value from 1 - 86,400 seconds. The default is 360 seconds.

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| retry-count <1-32>     | Configures the maximum number of times the BGP process is reset before being permanently shut down. Once shut down, the BGP process has to be started manually. The BGP process is reset if it is flooded with route entries that exceed the maximum number of routes configured for this device. <ul style="list-style-type: none"> <li>&lt;1-32&gt; – Specify a value from 1 - 32. The default is 5 routes.</li> </ul> |
| retry-timeout <1-3600> | Configures the duration, in seconds, the BGP process is temporarily shut down, before a reset of the process is attempted. <ul style="list-style-type: none"> <li>&lt;1-3600&gt; – Specify a value from 1 - 3600 seconds. The default is 60 seconds.</li> </ul>                                                                                                                                                          |

### Examples

```

nx9500-6C8809(config-profile NX9500Profile-router-bgp)#bgp-route-limit num-routes 10
nx9500-6C8809(config-profile NX9500Profile-router-bgp)#show context
router bgp
 bgp enable
 asn 1
 aggregate-address 116.117.118.0/24 as-set summary-only
 bgp neighbor 192.168.13.99
 remote-as 199
 maximum-prefix 9999 80 restart 50
 bgp-route-limit num-routes 10
nx9500-6C8809(config-profile NX9500Profile-router-bgp)#

```

### Related Commands

|                                                  |                                                                                         |
|--------------------------------------------------|-----------------------------------------------------------------------------------------|
| <code>no (bgp-router-config)</code> on page 1893 | Removes BGP route limitations configured. Use the no command to revert back to default. |
|--------------------------------------------------|-----------------------------------------------------------------------------------------|

### *distance (bgp-router-config)*

Configures administrative distance parameters. The distance parameter is a rating of the trustworthiness of a route. The higher the distance, lower is the trust rating. The distance can be set for each type of route indicating its trust rating.

#### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

#### Syntax

```
distance [<IP/M> <1-255> <BGP-ACL-NAME>|bgp <1-255> <1-255> <1-255>]
```

#### Parameters

```
distance [<IP/M> <1-255> <BGP-ACL-NAME>|bgp <1-255> <1-255> <1-255>]
```

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| distance <IP/M> <1-255> <BGP-ACL-NAME> | <p>Configures the default administrative distance, specified by the</p> <ul style="list-style-type: none"> <li>• &lt;1-255&gt; parameter, when the route's source IP address matches the specified IP prefix</li> <li>• &lt;IP/M&gt; – Specify the IP source prefix and prefix length.</li> <li>• &lt;1-255&gt; – Specify the distance from 1 - 255.</li> <li>• &lt;BGP-ACL-NAME&gt; – Optional. Specify the BGP access list name.</li> </ul>                                                                                      |
| bgp <1-255> <1-255> <1-255>            | <p>Configures the default administrative distance for different route types</p> <ul style="list-style-type: none"> <li>• &lt;1-255&gt; – Configures the default administrative distance for routes external to this AS. Specify a value from 1 - 255.</li> <li>• &lt;1-255&gt; – Configures the default administrative distance for routes internal to this AS. Specify a value from 1 - 255.</li> <li>• &lt;1-255&gt; – Configures the default administrative distance for local routes. Specify a value from 1 - 255.</li> </ul> |

### Examples

```

nx9500-6C8809(config-profile testNX9000-router-bgp)#distance bgp 200 100 200
nx9500-6C8809(config-profile testNX9000-router-bgp)#show context
router bgp
 bgp enable
 asn 1
 aggregate-address 116.117.118.0/24 as-set summary-only
 distance bgp 200 100 200
 bgp neighbor 192.168.13.99
 remote-as 199
 maximum-prefix 9999 80 restart 50
 bgp-route-limit num-routes 10
nx9500-6C8809(config-profile testNX9000-router-bgp)#

```

### Related Commands

|                                     |                                                            |
|-------------------------------------|------------------------------------------------------------|
| no (bgp-router-config) on page 1893 | Removes the administrative distance related configurations |
|-------------------------------------|------------------------------------------------------------|

### *ip (bgp-router-config)*

Configures the BGP default gateway's priority

#### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

#### Syntax

```
ip default-gateway priority <1-8000>
```

#### Parameters

```
ip default-gateway priority <1-8000>
```

|                                   |                                                                                                                                                                                                                                           |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| default-gateway priority <1-8000> | <p>Configures the default gateway's (acquired through BGP) priority</p> <ul style="list-style-type: none"> <li>• &lt;1-8000&gt; – Specify a value from 1 - 8000. The default is 7500. Lower the value, higher is the priority.</li> </ul> |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-profile testNX9000-router-bgp)#ip default-gateway priority 1
nx9500-6C8809(config-profile testNX9000-router-bgp)#show context
router bgp
 bgp enable
 asn 1
 ip default-gateway priority 1
 bgp-route-limit num-routes 10
nx9500-6C8809(config-profile testNX9000-router-bgpp)#
```

## Related Commands

|                                                  |                                               |
|--------------------------------------------------|-----------------------------------------------|
| <code>no (bgp-router-config)</code> on page 1893 | Removes the BGP default gateway configuration |
|--------------------------------------------------|-----------------------------------------------|

### *network (bgp-router-config)*

Configures the local network IP addresses and masks. These network addresses are broadcasted to neighboring BGP peers. You can configure a single IP address or a range of IP addresses in the A.B.C.D/M notation.

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

### Syntax

```
network <IP/M> {backdoor/pathlimit/route-map}
network <IP/M> {backdoor pathlimit <1-255>}
network <IP/M> {pathlimit <1-255>}
network <IP/M> {route-map <ROUTE-MAP-NAME>}
```

### Parameters

```
network <IP/M> {backdoor pathlimit <1-255>/pathlimit <1-255>/route-map <ROUTE-MAP-NAME>}
```

|                            |                                                                                                                                                                                                                                                                                                    |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| network <IP/M>             | Configures the local network's address in the A.B.C.D/M format <ul style="list-style-type: none"><li>• &lt;IP/M&gt; - Specify the network address.</li></ul>                                                                                                                                       |
| backdoor pathlimit <1-255> | Optional. Configures a BGP backdoor route. After configuring the backdoor route, you can optionally configure the as-path hop count limit attribute for this backdoor route. <ul style="list-style-type: none"><li>• pathlimit &lt;1-255&gt; - Specify the hop count limit from 1 - 255.</li></ul> |
| pathlimit <1-255>          | Optional. Configures the maximum path limit for this AS <ul style="list-style-type: none"><li>• &lt;1-255&gt; - Specify the hop count limit from 1 - 255.</li></ul>                                                                                                                                |
| route-map <ROUTE-MAP-NAME> | Optional. Associates a BGP route map with this local network. When applied, the route-map values take precedence <ul style="list-style-type: none"><li>• &lt;ROUTE-MAP-NAME&gt; - Specify the route map name.</li></ul>                                                                            |

## Examples

```
nx9500-6C8809(config-profile testNX9000-router-bgp)#network 192.168.13.0/24 backdoor
pathlimit 200
nx9500-6C8809(config-profile testNX9000-router-bgp)#show context
router bgp
 bgp enable
```

```

asn 1
aggregate-address 116.117.118.0/24 as-set summary-only
distance bgp 200 100 200
bgp neighbor 192.168.13.99
 remote-as 199
 maximum-prefix 9999 80 restart 50
network 1.2.3.0/24
network 192.168.13.0/24 backdoor pathlimit 200
bgp-route-limit num-routes 10
nx9500-6C8809(config-profile testNX9000-router-bgp)#

```

### Related Commands

|                                                  |                                               |
|--------------------------------------------------|-----------------------------------------------|
| <code>no (bgp-router-config)</code> on page 1893 | Removes the list of local networks configured |
|--------------------------------------------------|-----------------------------------------------|

### *route-redistribute (bgp-router-config)*

Enables redistribution of routes learnt from other routing protocols into BGP.

Large ISP networks using multiple routing protocols, need to enable redistribution of routes across routing protocols. Routing protocols differ in their basic characteristics, such as metrics, administrative distance, classful and classless capabilities, etc. When enabling redistribution, these differences have to be taken into consideration.

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

### Syntax

```
route-redistribute [connected|kernel|ospf|static] {metric <0-4294967295>/route-map <ROUTE-MAP-NAME>}
```

### Parameters

```
route-redistribute [connected|kernel|ospf|static] {metric <0-4294967295>/route-map <ROUTE-MAP-NAME>}
```

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| route-redistribute | Redistributes routes learnt from other protocols                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| connected          | Redistributes directly connected routes <ul style="list-style-type: none"> <li>• metric &lt;0-4294967295&gt; - Optional. Specify the metric for the redistributed routes. route-map</li> <li>• &lt;ROUTE-MAP-NAME&gt; - Optional. Specifies the route map name. The route map defines the match criteria based on which routes are filtered before redistribution. For more information on route maps, see <a href="#">match</a>.</li> </ul>                                                            |
| kernel             | Redistributes kernel routes. These are routes that are neither connected, nor static, nor dynamic. <ul style="list-style-type: none"> <li>• metric &lt;0-4294967295&gt; - Optional. Specify the metric for the redistributed routes.</li> <li>• route-map &lt;ROUTE-MAP-NAME&gt; - Optional. Specifies the route map name. The route map defines the match criteria based on which routes are filtered before redistribution. For more information on route maps, see <a href="#">match</a>.</li> </ul> |

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ospf   | <p>Redistributes OSPF routes</p> <ul style="list-style-type: none"> <li>metric &lt;0-4294967295&gt; - Optional. Specify the metric for the redistributed routes.</li> <li>route-map &lt;ROUTE-MAP-NAME&gt; - Optional. Specifies the route map name. The route map defines the match criteria based on which routes are filtered before redistribution. For more information on route maps, see <a href="#">match</a>.</li> </ul>   |
| static | <p>Redistributes static routes</p> <ul style="list-style-type: none"> <li>metric &lt;0-4294967295&gt; - Optional. Specify the metric for the redistributed routes.</li> <li>route-map &lt;ROUTE-MAP-NAME&gt; - Optional. Specifies the route map name. The route map defines the match criteria based on which routes are filtered before redistribution. For more information on route maps, see <a href="#">match</a>.</li> </ul> |

### Examples

```

nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#route-redistribute
connected metric 200
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#show context
router bgp
 bgp enable
 asn 1
 aggregate-address 116.117.118.0/24 as-set summary-only
 bgp neighbor 192.168.13.99
 remote-as 199
 maximum-prefix 9999 80 restart 50
 bgp neighbor 192.168.13.199
 remote-as 1
 use route-map UnSupMap_01 in
 route-redistribute connected metric 200
 bgp-route-limit num-routes 10 reset-time 360
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#

```

### Related Commands

|                                                     |                                                                                |
|-----------------------------------------------------|--------------------------------------------------------------------------------|
| <a href="#">no (bgp-router-config)</a> on page 1893 | Disables redistribution of routes learnt from other routing protocols into BGP |
|-----------------------------------------------------|--------------------------------------------------------------------------------|

### *timers (bgp-router-config)*

Enables adjustment of keepalive and holdtime intervals

#### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

#### Syntax

```
timers bgp <0-65535> <0-65535>
```

#### Parameters

```
timers bgp <0-65535> <0-65535>
```



|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>timers bgp &lt;0-65535&gt; &lt;0-65535&gt; Configures the keepalive and holdtime interval in seconds</p> <ul style="list-style-type: none"> <li>• &lt;0-65535&gt; - Specify a keepalive interval from 0 - 65535 seconds. It is the interval, in seconds, between two successive keepalive packets exchanged with this router and its neighbor to keep the TCP connection alive.</li> <li>• &lt;0-65535&gt; - Specify a holdtime value from 0 - 65535 seconds. This is the time this router will wait without receiving a keepalive packet from its neighbor before declaring it dead. If the time since the last keepalive packet received (from its neighbor) exceeds the value set here, the neighbor is declared dead.</li> </ul> |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```

nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#timers bgp 100 100
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#show context
router bgp
 bgp enable
 asn 1
 aggregate-address 116.117.118.0/24 as-set summary-only
 bgp neighbor 192.168.13.199
 remote-as 1
 use route-map UnSupMap_01 in
 bgp neighbor 192.168.13.99
 remote-as 199
 maximum-prefix 9999 80 restart 50
 timers bgp 100 100
 bgp-route-limit num-routes 10 reset-time 360
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#

```

### Related Commands

|                                                     |                               |
|-----------------------------------------------------|-------------------------------|
| <a href="#">no (bgp-router-config)</a> on page 1893 | Reverts BGP timers to default |
|-----------------------------------------------------|-------------------------------|

### *no (bgp-router-config)*

Removes the BGP router settings

#### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

#### Syntax

```
no [aggregate-address|bgp|bgp-route-limit|distance|ip|network|route-redistribute|timers]
```

#### Parameters

```
no <PARAMETERS>
```

|                                    |                                                                |
|------------------------------------|----------------------------------------------------------------|
| <code>no &lt;PARAMETERS&gt;</code> | Removes the BGP router settings based on the parameters passed |
|------------------------------------|----------------------------------------------------------------|

### Examples

The following example shows the BGP router settings before the 'no' commands have been executed:

```

nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#show context
router bgp
 bgp enable

```

```

asn 1
aggregate-address 116.117.118.0/24 as-set summary-only
bgp neighbor 192.168.13.199
 remote-as 1
 use route-map UnSupMap_01 in
bgp neighbor 192.168.13.99
 remote-as 199
 maximum-prefix 9999 80 restart 50
bgp-route-limit num-routes 10 reset-time 360
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#no bgp neighbor 192.168.13.99
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#no aggregate-address
116.117.118.0/24
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#no bgp-route-limit

```

The following example shows the BGP router settings after the 'no' commands have been executed:

```

nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#show context
router bgp
 bgp enable
 asn 1
 bgp neighbor 192.168.13.199
 remote-as 1
 use route-map UnSupMap_01 in
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#

```

## bgp neighbor-config

BGP enabled devices connected through an established TCP connection are referred to as BGP peers or neighbors. To establish a TCP connection, BGP routers exchange open messages containing the following information: AS number, BGP version running, BGP router ID, and timer values (keepalive and holdtime). Once these values are accepted by both devices, the connection is established and the routers become neighbors. With the TCP connection established the BGP neighbors begin sharing routing information and updates. A failure in the establishment of the TCP connection indicates that the routers are not neighbors and cannot exchange routing information.

Use the (profile/device-config) instance to configure BGP neighbors.

To navigate to the BGP neighbor configuration instance, use the following commands:

```

<DEVICE>(config)#profile <PROFILE-NAME>
<DEVICE>(config-profile <PROFILE-NAME>)#router bgp
<DEVICE>(config-profile <PROFILE-NAME>-router-bgp)#?
<DEVICE>(config-profile <PROFILE-NAME>-router-bgp)#bgp neighbor ?
 A.B.C.D IP address of the bgp neighbor

<DEVICE>(config-profile <PROFILE-NAME>-router-bgp)#
<DEVICE>(config-profile <PROFILE-NAME>-router-bgp)#bgp neighbor <IP>
<DEVICE>(config-profile <PROFILE-NAME>-router-bgp-neighbor-<IP>)#?
Router BGP Neighbor Mode commands:
 activate Enable the Address Family for this Neighbor
 (EXPERIMENTAL)
 advertisement-interval Minimum interval between BGP routing updates
 allowas-in Accept as-path with my AS present in it
 (EXPERIMENTAL)
 attribute-unchanged BGP attribute is propagated unchanged to this
 neighbor (EXPERIMENTAL)
 capability Advertise capability to the peer
 default-originate Originate default route to this neighbor
 description Neighbor specific description
 disable-connected-check One-hop away EBGp peer using loopback address
 (EXPERIMENTAL)

```

```

dont-capability-negotiate Do not perform capability negotiation
 (EXPERIMENTAL)
ebgp-multihop Allow EBGp neighbors not on directly connected
 networks
enforce-multihop Enforce EBGp neighbors perform multihop
 (EXPERIMENTAL)
local-as Specify a local-as number (EXPERIMENTAL)
maximum-prefix Maximum number of prefix accept from this peer
next-hop-self Disable the next hop calculation for this
 neighbor
no Negate a command or set its defaults
override-capability Override capability negotiation result
passive Don't send open messages to this neighbor
password Set a password
peer-group Set peer-group for this neighbor (EXPERIMENTAL)
port Neighbor's BGP port (EXPERIMENTAL)
remote-as Specify a BGP neighbor
remove-private-as Remove private AS number from outbound updates
 (EXPERIMENTAL)
route-server-client Configure a neighbor as Route Server client
 (EXPERIMENTAL)
send-community Send Community attribute to this neighbor
shutdown Administratively shut down this neighbor
soft-reconfiguration Per neighbor soft reconfiguration
strict-capability-match Strict capability negotiation match
 (EXPERIMENTAL)
timers BGP per neighbor timers
unsuppress-map Route-map to selectively unsuppress suppressed
 routes
update-source Source of routing updates
use Set setting to use
weight Set default weight for routes from this neighbor

clrscr Clears the display screen
commit Commit all changes made in this session
do Run commands from Exec mode
end End current mode and change to EXEC mode
exit End current mode and down to previous mode
help Description of the interactive help system
revert Revert changes
service Service Commands
show Show running system information
write Write running configuration to memory or terminal

```

```
<DEVICE>(config-profile <PROFILE-NAME>-router--bgp-neighbor-<IP>)#
```

The following table summarizes BGP deny/permit route map rules configuration mode commands:

**Table 78: BGP-Neighbor Config Mode Commands**

| Command                                                                   | Description                                                                                          |
|---------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| <a href="#">activate (bgp-neighbor-config)</a> on page 1897               | Enables an address family for this neighbor (EXPERIMENTAL)                                           |
| <a href="#">advertisement-interval (bgp-neighbor-config)</a> on page 1897 | Configures the minimum interval between two consecutive BGP router updates                           |
| <a href="#">allowas-in (bgp-neighbor-config)</a> on page 1898             | Enables re-advertisement of all prefixes containing duplicate ASNs (EXPERIMENTAL)                    |
| <a href="#">attribute-unchanged (bgp-neighbor-config)</a> on page 1899    | Enables the propagation of BGP attribute values unchanged to this neighbor BGP device (EXPERIMENTAL) |

**Table 78: BGP-Neighbor Config Mode Commands (continued)**

| Command                                                                      | Description                                                                                                                                                    |
|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">capability (bgp-neighbor-config)</a> on page 1900                | Enables the advertisement of capability (dynamic and ORF) to BGP peers                                                                                         |
| <a href="#">default-originate (bgp-neighbor-config)</a> on page 1900         | Enables the sending of the default route to BGP neighbors. It also allows the configuration of the default route.                                              |
| <a href="#">description (bgp-neighbor-config)</a> on page 1901               | Configures a description for a BGP neighbor device                                                                                                             |
| <a href="#">disable-connected-check (bgp-neighbor-config)</a> on page 1902   | Enables one-hop away EBGP peer using loop back address (EXPERIMENTAL)                                                                                          |
| <a href="#">dont-capability-negotiate (bgp-neighbor-config)</a> on page 1902 | Disables capability negotiation with BGP neighbors (EXPERIMENTAL)                                                                                              |
| <a href="#">ebgp-multihop (bgp-neighbor-config)</a> on page 1903             | Enables eBGP Multihop on this BGP neighbor, and configures the maximum number of hops that can be between eBGP neighbors not directly connected to each other. |
| <a href="#">enforce-multihop (bgp-neighbor-config)</a> on page 1904          | Forces EBGP neighbors to perform multi-hop checks (EXPERIMENTAL)                                                                                               |
| <a href="#">local-as (bgp-neighbor-config)</a> on page 1904                  | Configures this neighbor's local AS number. Also enables the prepending of this AS number in route updates. (EXPERIMENTAL)                                     |
| <a href="#">maximum-prefix (bgp-neighbor-config)</a> on page 1905            | Configures the maximum number of prefixes that can be received from a BGP neighbor                                                                             |
| <a href="#">next-hop-self (bgp-neighbor-config)</a> on page 1906             | Enables next-hop calculation for this neighbor                                                                                                                 |
| <a href="#">override-capability (bgp-neighbor-config)</a> on page 1907       | Enables the overriding of capability negotiation results                                                                                                       |
| <a href="#">passive (bgp-neighbor-config)</a> on page 1908                   | Enables this BGP neighbor device (or devices using this profile) as passive                                                                                    |
| <a href="#">password (bgp-neighbor-config)</a> on page 1909                  | Sets a password for this BGP neighbor device (or devices using this profile)                                                                                   |
| <a href="#">peer-group (bgp-neighbor-config)</a> on page 1909                | Sets the peer group for this BGP neighbor device (or devices using this profile) (EXPERIMENTAL)                                                                |
| <a href="#">port (bgp-neighbor-config)</a> on page 1910                      | Configures a non-standard BGP port for this BGP neighbor (EXPERIMENTAL)                                                                                        |
| <a href="#">remote-as (bgp-neighbor-config)</a> on page 1911                 | Configures the ASN for this neighbor BGP device (or devices using this profile)                                                                                |
| <a href="#">remove-private-as (bgp-neighbor-config)</a> on page 1912         | Removes the private ASN from outbound updates (EXPERIMENTAL)                                                                                                   |
| <a href="#">route-server-client (bgp-neighbor-config)</a> on page 1913       | Enables this BGP neighbor device (or devices using this profile) to act as a route server client (EXPERIMENTAL)                                                |
| <a href="#">send-community (bgp-neighbor-config)</a> on page 1914            | Enables sending of the community attribute to the BGP neighbor                                                                                                 |
| <a href="#">shutdown (bgp-neighbor-config)</a> on page 1915                  | Shuts down this BGP neighbor device (or devices using this profile)                                                                                            |

**Table 78: BGP-Neighbor Config Mode Commands (continued)**

| Command                                                                    | Description                                                                                                                                                                                   |
|----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">soft-reconfiguration (bgp-neighbor-config)</a> on page 1915    | Enables storing of updates for inbound soft reconfiguration                                                                                                                                   |
| <a href="#">strict-capability-match (bgp-neighbor-config)</a> on page 1916 | Enables a strict capability match before allowing a neighbor BGP peer to open a connection (EXPERIMENTAL)                                                                                     |
| <a href="#">timers (bgp-neighbor-config)</a> on page 1916                  | Configures this BGP neighbor's keepalive and holdtime durations                                                                                                                               |
| <a href="#">unsuppress-map (bgp-neighbor-config)</a> on page 1918          | Uses a route-map that selectively un suppresses routes that have been suppressed using the aggregate-address command                                                                          |
| <a href="#">update-source (bgp-neighbor-config)</a> on page 1918           | Allows BGP sessions to use any operational interface to establish the TCP connection with this neighbor                                                                                       |
| <a href="#">use (bgp-neighbor-config)</a> on page 1919                     | Configures filters for this neighbor. These filters are BGP IP ACL, IP prefix list, AS path list, and route map. Based on the filters used, updates received from this neighbor are filtered. |
| <a href="#">weight (bgp-neighbor-config)</a> on page 1920                  | Configures a weight for all routes learned from this BGP neighbor                                                                                                                             |
| <a href="#">no (bgp-neighbor-config)</a> on page 1921                      | Removes this BGP neighbor's settings, or reverts them back to default                                                                                                                         |

*activate (bgp-neighbor-config)*

Enables an address family for this neighbor. This option is enabled by default.

**Supported in the following platforms:**

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

**Syntax**

activate

**Parameters**

None

**Examples**

```
nx9500-6C8809(config-profile testNX9500-router-bgp-neighbor-192.168.13.99)#activate
```

**Related Commands**

|                                                       |                                                   |
|-------------------------------------------------------|---------------------------------------------------|
| <a href="#">no (bgp-neighbor-config)</a> on page 1921 | Disables an address family for this BGP neighbor. |
|-------------------------------------------------------|---------------------------------------------------|

*advertisement-interval (bgp-neighbor-config)*

Configures the minimum interval, in seconds, between two consecutive BGP router updates

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

### Syntax

```
advertisement-interval <0-600>
```

### Parameters

```
advertisement-interval <0-600>
```

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| advertisement-interval <0-600> | Configures the minimum interval, in seconds, between two consecutive BGP router updates. Sending too many router updates creates flapping of routes leading to possible disruptions. Specify a minimum interval so that the BGP routing updates are sent after the set interval. <ul style="list-style-type: none"><li>• &lt;0-600&gt; - Specify a value from 0 - 600 seconds. The default is 5 seconds.</li></ul> |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)# advertisement-interval 100
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show
context
 bgp neighbor 192.168.13.99
 advertisement-interval 100
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

### Related Commands

|                                                    |                                                                                                |
|----------------------------------------------------|------------------------------------------------------------------------------------------------|
| <code>no (bgp-neighbor-config) on page 1921</code> | Reverts the minimum interval between two consecutive BGP router updates to default (5 seconds) |
|----------------------------------------------------|------------------------------------------------------------------------------------------------|

### *allows-in (bgp-neighbor-config)*

Enables re-advertisement of all prefixes containing duplicate ASNs. Use this command to configure the maximum number of times an ASN is advertised. This option is disabled by default.

When enabled, PE (Provider Edge) routers can re-advertise all prefixes containing duplicate ASNs. This creates a pair of VRF (VPN Routing/Forwarding) instances on each PE router to receive and re-advertise prefixes. The PE router receives prefixes with ASNs from all PE routers and advertises to its neighbor PE routers on one VRF. The other VRF receives prefixes with ASNs from the CE (Customer Edge) routers and re-advertises them to all PE routers in the configuration.

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

### Syntax

```
allows-in <1-10>
```

### Parameters

```
allows-in <1-10>
```

allows-in <1-10>

Enables and configures the maximum number of times an ASN is advertised.

- <1-10> – Specify a value from 1 - 10.

### Examples

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#allows-in 10
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show context
 bgp neighbor 192.168.13.99
 advertisement-interval 100
 allows-in 10
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

### Related Commands

[no \(bgp-neighbor-config\)](#) on page 1921

Disables re-advertisement of all prefixes containing duplicate ASNs.

### *attribute-unchanged (bgp-neighbor-config)*

Enables propagation of BGP attribute values unchanged to this neighbor BGP device. The BGP attributes are: as-path, med, and next-hop.

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

### Syntax

```
attribute-unchanged { (as-path|med|next-hop) }
```

### Parameters

```
attribute-unchanged { (as-path|med|next-hop) }
```

attribute-unchanged

Enables the propagation of the following BGP attribute values unchanged:

- as-path – Optional. Enables propagation of AS path BGP attribute unchanged to this neighbor BGP device. This option is disabled by default.
- med – Optional. Enables propagation of MED BGP attribute unchanged to this neighbor BGP device. This option is disabled by default.
- next-hop – Optional. Enables propagation of the next-hop BGP attribute value unchanged to this neighbor BGP device. This option is disabled by default.

### Examples

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#attribute-
unchanged as-path
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show
context
 bgp neighbor 192.168.13.99
 advertisement-interval 100
 allows-in 10
 attribute-unchanged as-path
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

## Related Commands

|                                                    |                                                                                     |
|----------------------------------------------------|-------------------------------------------------------------------------------------|
| <code>no (bgp-neighbor-config)</code> on page 1921 | Disables propagation of BGP attribute values unchanged to this neighbor BGP device. |
|----------------------------------------------------|-------------------------------------------------------------------------------------|

### *capability (bgp-neighbor-config)*

Enables the advertisement of capability (dynamic and ORF) to BGP peers

#### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

#### Syntax

```
capability [dynamic|orf]
capability dynamic
capability orf prefix-list [both|receive|send]
```

#### Parameters

```
capability dynamic
```

|                                 |                                                                                                                                                                                                                                             |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>capability dynamic</code> | Enables the advertisement of dynamic capability<br>Enable this option to show a neighbor device's capability to advertise or withdraw and address capability to other peers in a non-disruptive manner. This option is disabled by default. |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
capability orf prefix-list [both|receive|send]
```

|                                                             |                                                                                                              |
|-------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| <code>capability orf prefix-list [both receive send]</code> | Enables the advertisement of Outbound Router Filtering (ORF) capability. This option is disabled by default. |
|-------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|

#### Examples

#### Related Commands

---

### *default-originate (bgp-neighbor-config)*

Enables the sending of the default route to BGP neighbors. It also allows the configuration of the default route. When enabled and configured, local BGP routers send the default route 0.0.0.0 (or a route map specified route) to its neighbor for use as the default route.

#### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

#### Syntax

```
default-originate {route-map <BGP-ROUTE-MAP-NAME>}
```



## Parameters

default-originate {route-map <BGP-ROUTE-MAP-NAME>}

|                                                       |                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| default-originate<br>{route-map <BGP-ROUTE-MAP-NAME>} | Enables default originate on this BGP neighbor. This option is disabled by default. <ul style="list-style-type: none"><li>route-map &lt;BGP-ROUTE-MAP&gt; – Optional. Use this keyword to specify a route map to use as the default originate route.</li></ul> <p><b>Note:</b> If no route-map is specified, the default route 0.0.0.0 is sent.</p> |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#default-originate
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show context
 bgp neighbor 192.168.13.99
 advertisement-interval 100
 allowas-in 10
 attribute-unchanged as-path
 capability orf prefix-list both
 default-originate
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

## Related Commands

|                                       |                                                        |
|---------------------------------------|--------------------------------------------------------|
| no (bgp-neighbor-config) on page 1921 | Disables sending of the default route to BGP neighbors |
|---------------------------------------|--------------------------------------------------------|

*description (bgp-neighbor-config)*

Configures a description for this BGP neighbor device

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

## Syntax

description neighbor <LINE>

## Parameters

description neighbor <LINE>

|                             |                                                                                       |
|-----------------------------|---------------------------------------------------------------------------------------|
| description neighbor <LINE> | Specify a description for this BGP neighbor device (should not exceed 80 characters). |
|-----------------------------|---------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#description
neighbor "This neighbor is an external AS neighbor"
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show context
 bgp neighbor 192.168.13.99
 advertisement-interval 100
 allowas-in 10
 attribute-unchanged as-path
 capability orf prefix-list both
 default-originate
```

```
description neighbor "This neighbor is an external AS neighbor"
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

### Related Commands

|                                                    |                                         |
|----------------------------------------------------|-----------------------------------------|
| <code>no (bgp-neighbor-config)</code> on page 1921 | Removes this BGP neighbor's description |
|----------------------------------------------------|-----------------------------------------|

### *disable-connected-check (bgp-neighbor-config)*

Enables one-hop away eBGP peer using loop back address. This option is disabled by default.

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

### Syntax

```
disable-connected-check
```

### Parameters

None

### Examples

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#disable-
connected-check
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show context
 bgp neighbor 192.168.13.99
 advertisement-interval 100
 allowas-in 10
 attribute-unchanged as-path
 capability orf prefix-list both
 default-originate
 description neighbor "This neighbor is an external AS neighbor"
 disable-connected-check
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

### Related Commands

|                                                    |                                                         |
|----------------------------------------------------|---------------------------------------------------------|
| <code>no (bgp-neighbor-config)</code> on page 1921 | Disables one-hop away eBGP peer using loop back address |
|----------------------------------------------------|---------------------------------------------------------|

### *dont-capability-negotiate (bgp-neighbor-config)*

Disables capability negotiation with BGP neighbors. This is to allow compatibility with older BGP versions that have no capability parameters used in the open messages between peers. Capability negotiation is enabled by default.

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

### Syntax

```
dont-capability-negotiate
```

## Parameters

None

## Examples

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#dont-capability-
negotiate
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show context
 bgp neighbor 192.168.13.99
 advertisement-interval 100
 allowas-in 10
 attribute-unchanged as-path
 capability orf prefix-list both
 default-originate
 description neighbor "This neighbor is an external AS neighbor"
 disable-connected-check
 dont-capability-negotiate
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

## Related Commands

[no \(bgp-neighbor-config\)](#) on page 1921

Enables capability negotiation with BGP neighbors

### *ebgp-multihop (bgp-neighbor-config)*

Enables eBGP Multihop on this BGP neighbor. When enabled, allows neighbor connection to be established between two eBGP neighbors that are not directly connected to each other. Use this command to configure the maximum number of hops possible between two such eBGP neighbors. This option is disabled by default.

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

## Syntax

```
ebgp-multihop <1-255>
```

## Parameters

```
ebgp-multihop <1-255>
```

`ebgp-multihop <1-255>`

Configures the maximum number of hops that can be between eBGP neighbors not directly connected to each other.

- `<1-255>` - Specify a value from 1 - 255. The default is 255.

## Examples

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#ebgp-multihop 20
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show context
 bgp neighbor 192.168.13.99
 advertisement-interval 100
 allowas-in 10
 attribute-unchanged as-path
 capability orf prefix-list both
 default-originate
 description neighbor "This neighbor is an external AS neighbor"
 disable-connected-check
```

```
dont-capability-negotiate
ebgp-multihop 20
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

### Related Commands

|                                                    |                                             |
|----------------------------------------------------|---------------------------------------------|
| <code>no (bgp-neighbor-config)</code> on page 1921 | Disables eBGP Multihop on this BGP neighbor |
|----------------------------------------------------|---------------------------------------------|

### *enforce-multihop (bgp-neighbor-config)*

Forces eBGP neighbors to perform multi-hop checks. A multihop route is a route to external peers on indirectly connected networks. When enforced, eBGP neighbors perform multi-hop check. This option is disabled by default.

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

### Syntax

```
enforce-multihop
```

### Parameters

None

### Examples

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#enforce-multihop
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show context
 bgp neighbor 192.168.13.99
 advertisement-interval 100
 allowas-in 10
 attribute-unchanged as-path
 capability orf prefix-list both
 default-originate
 description neighbor "This neighbor is an external AS neighbor"
 disable-connected-check
 dont-capability-negotiate
 ebgp-multihop 20
 enforce-multihop
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

### Related Commands

|                                                    |                                               |
|----------------------------------------------------|-----------------------------------------------|
| <code>no (bgp-neighbor-config)</code> on page 1921 | Disables enforcement of multihop route checks |
|----------------------------------------------------|-----------------------------------------------|

### *local-as (bgp-neighbor-config)*

Configures this neighbor's local AS number

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

## Syntax

```
local-as <1-4294967295> {no-prepend}
```

## Parameters

```
local-as <1-4294967295> {no-prepend}
```

|                                                       |                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>local-as &lt;1-4294967295&gt; {no-prepend}</pre> | <p>Configures the local AS number</p> <ul style="list-style-type: none"><li>• &lt;1-4292967295&gt; – Specify a value from 1 - 4294967295.</li><li>• no-prepend – Optional. Select to enable. When enabled, the local AS number is not prepended to route updates from eBGP peers. AS numbers are prepended to route updates by default.</li></ul> |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#local-as 20 no-prepend
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show context
 bgp neighbor 192.168.13.99
 advertisement-interval 100
 allowas-in 10
 attribute-unchanged as-path
 capability orf prefix-list both
 default-originate
 description neighbor "This neighbor is an external AS neighbor"
 disable-connected-check
 dont-capability-negotiate
 ebgp-multihop 20
 enforce-multihop
 local-as 20 no-prepend
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

## Related Commands

|                                                  |                                                                                                               |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| <pre>no (bgp-neighbor-config) on page 1921</pre> | <p>Removes the local AS number. And also reverts prepending of AS numbers to default (allows prepending).</p> |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------|

### *maximum-prefix (bgp-neighbor-config)*

Configures the maximum number of prefixes that can be received from a BGP neighbor. This option is disabled by default.

#### **Supported in the following platforms:**

- Wireless Controllers – RFS 4000
- Service Platforms – NX 95XX, NX 96XX

## Syntax

```
maximum-prefix <1-4294967295> {(<1-100>|restart <1-65535>|warning-only)}
```

## Parameters

```
maximum-prefix <1-4294967295> {(<1-100>|restart <1-65535>|warning-only)}
```

|                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>maximum-prefix &lt;1-4294967295&gt;</pre> | <p>Configures the maximum number of prefixes that can be received from a BGP neighbor</p> <ul style="list-style-type: none"> <li>• &lt;1-4294967295&gt; – Specify a value for 1 - 4294967295.</li> <li>• &lt;1-100&gt; – Optional. Sets the threshold limit for generating a log message. This value represents a percentage of the maximum-prefix configured in the preceding step. When this value is reached, a log entry is generated. For example if the maximum-prefix is set to 100 and threshold limit is set to 65, then after receiving 65 prefixes, a log entry is generated. This option is disabled by default.</li> <li>• restart &lt;1-65535&gt; – Optional. Restarts BGP peer connection once the maximum-prefix limit specified is exceeded. For example, If the value specified is 10, then after receiving 10 prefixes from the neighbor, the system restarts the connection with that neighbor. Specify a value from 1 - 65535. This option is disabled by default.</li> <li>• warning-only – Configure to enable. When the maximum-prefix limit is exceeded, the connection is restarted. However, when this option is enabled, the connection is not restarted and an event is generated instead. This option is disabled by default.</li> </ul> |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Examples

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#maximum-prefix
400 50 warning-only
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show con
 bgp neighbor 192.168.13.99
 advertisement-interval 100
 allowas-in 10
 attribute-unchanged as-path
 capability orf prefix-list both
 default-originate
 description neighbor "This neighbor is an external AS neighbor"
 disable-connected-check
 dont-capability-negotiate
 ebgp-multihop 20
 enforce-multihop
 local-as 20 no-prepend
 maximum-prefix 400 50 warning-only
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

### Related Commands

|                                                    |                                                                  |
|----------------------------------------------------|------------------------------------------------------------------|
| <code>no (bgp-neighbor-config)</code> on page 1921 | Removes the maximum prefix settings configured for this neighbor |
|----------------------------------------------------|------------------------------------------------------------------|

### *next-hop-self (bgp-neighbor-config)*

Enables next-hop calculation for this neighbor. This option is disabled by default. When enabled, this device (or devices using this profile) are configured as the next hop for the BGP speaking neighbor or peer group. This allows the BGP device to change the next hop information that is sent to iBGP peers. The next hop address is set to the IP address of the interface used to communicate with the eBGP neighbor.

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

## Syntax

next-hop-self

## Parameters

None

## Examples

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#next-hop-self
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show context
 bgp neighbor 192.168.13.99
 advertisement-interval 100
 allowas-in 10
 attribute-unchanged as-path
 capability orf prefix-list both
 default-originate
 description neighbor "This neighbor is an external AS neighbor"
 disable-connected-check
 dont-capability-negotiate
 ebgp-multihop 20
 enforce-multihop
 local-as 20 no-prepend
 maximum-prefix 400 50 warning-only
 next-hop-self
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

## Related Commands

|                                                    |                                                                       |
|----------------------------------------------------|-----------------------------------------------------------------------|
| <code>no (bgp-neighbor-config)</code> on page 1921 | Disables next-hop calculation for this neighbor (this is the default) |
|----------------------------------------------------|-----------------------------------------------------------------------|

### *override-capability (bgp-neighbor-config)*

Enables the overriding of capability negotiation results. This option is disabled by default.

#### **Supported in the following platforms:**

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

## Syntax

override-capability

## Parameters

None

## Examples

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#override-
capability
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show context
 bgp neighbor 192.168.13.99
 advertisement-interval 100
 allowas-in 10
 attribute-unchanged as-path
 capability orf prefix-list both
 default-originate
 description neighbor "This neighbor is an external AS neighbor"
```

```

disable-connected-check
dont-capability-negotiate
ebgp-multihop 20
enforce-multihop
local-as 20 no-prepend
maximum-prefix 400 50 warning-only
next-hop-self
override-capability
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#

```

## Related Commands

|                                                    |                                                           |
|----------------------------------------------------|-----------------------------------------------------------|
| <code>no (bgp-neighbor-config)</code> on page 1921 | Disables the overriding of capability negotiation results |
|----------------------------------------------------|-----------------------------------------------------------|

### *passive (bgp-neighbor-config)*

Enables this BGP neighbor device (or devices using this profile) as passive. When enabled, local devices do not attempt to open a connection to passive BGP neighbors. This option is disabled by default.

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

### Syntax

```
passive
```

### Parameters

None

### Examples

```

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#passive
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show context
 bgp neighbor 192.168.13.99
 advertisement-interval 100
 allowas-in 10
 attribute-unchanged as-path
 capability orf prefix-list both
 default-originate
 description neighbor "This neighbor is an external AS neighbor"
 disable-connected-check
 dont-capability-negotiate
 ebgp-multihop 20
 enforce-multihop
 local-as 20 no-prepend
 maximum-prefix 400 50 warning-only
 next-hop-self
 override-capability
 passive
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#

```

## Related Commands

|                                                    |                                                                              |
|----------------------------------------------------|------------------------------------------------------------------------------|
| <code>no (bgp-neighbor-config)</code> on page 1921 | Disables this BGP neighbor device (or devices using this profile) as passive |
|----------------------------------------------------|------------------------------------------------------------------------------|



### *password (bgp-neighbor-config)*

Sets a password for this BGP neighbor device (or devices using this profile). When configured, this password is used for MD5 (Message Digest 5) authentication between two BGP peers connected over TCP. To enable MD5 authentication between two BGP peers, configure both with the same password.

#### **Supported in the following platforms:**

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

#### **Syntax**

```
password neighbor <LINE>
```

#### **Parameters**

```
password neighbor <LINE>
```

|                          |                      |
|--------------------------|----------------------|
| password neighbor <LINE> | Specify the password |
|--------------------------|----------------------|

#### **Examples**

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#password
neighbor eBGPneighbor@300
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)# show context
 bgp neighbor 192.168.13.99
 advertisement-interval 100
 allowas-in 10
 attribute-unchanged as-path
 capability orf prefix-list both
 default-originate
 description neighbor "This neighbor is an external AS neighbor"
 disable-connected-check
 dont-capability-negotiate
 ebgp-multihop 20
 enforce-multihop
 local-as 20 no-prepend
 maximum-prefix 400 50 warning-only
 next-hop-self
 override-capability
 passive
 password neighbor eBGPneighbor@300
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

#### **Related Commands**

|                                                       |                                                   |
|-------------------------------------------------------|---------------------------------------------------|
| <a href="#">no (bgp-neighbor-config)</a> on page 1921 | Removes the password configured for this neighbor |
|-------------------------------------------------------|---------------------------------------------------|

### *peer-group (bgp-neighbor-config)*

Sets the peer group for this BGP neighbor device (or devices using this profile). Peer groups are a set of BGP neighbors with the same update policies. This facilitates the updates of various policies, such as, distribute lists and filter lists.

#### **Supported in the following platforms:**

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

## Syntax

```
peer-group <PEER-GROUP-NAME>
```

## Parameters

```
peer-group <PEER-GROUP-NAME>
```

|                              |                                                                                                                                                                                                                                                            |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| peer-group <PEER-GROUP-NAME> | Specify the peer group name. Once specified, this neighbor device becomes a member of the peer group identified by the <PEER-GROUP-NAME> keyword. <ul style="list-style-type: none"><li>• &lt;PEER-GROUP-NAME&gt; - Specify the peer group name.</li></ul> |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#peer-group
eBGPPeerGrp1
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show context
 bgp neighbor 192.168.13.99
 advertisement-interval 100
 peer-group eBGPPeerGrp1
 allow-as-in 10
 attribute-unchanged as-path
 capability orf prefix-list both
 default-originate
 description neighbor "This neighbor is an external AS neighbor"
 disable-connected-check
 dont-capability-negotiate
 ebgp-multihop 20
 enforce-multihop
 local-as 20 no-prepend
 maximum-prefix 400 50 warning-only
 next-hop-self
 override-capability
 passive
 password neighbor eBGPneighbor@300
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

## Related Commands

|                                                    |                                                                                    |
|----------------------------------------------------|------------------------------------------------------------------------------------|
| <code>no (bgp-neighbor-config)</code> on page 1921 | Removes the peer group configuration. This neighbor peer group setting is removed. |
|----------------------------------------------------|------------------------------------------------------------------------------------|

### *port (bgp-neighbor-config)*

Configures a non-standard BGP port for this BGP neighbor. By default BGP uses port 179. Use this command to set a non standard port for this BGP neighbor.

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

## Syntax

```
port <0-65535>
```

## Parameters

```
port <0-65535>
```

```
port <0-65535>
```

Specify a value from 0 - 65535.

### Examples

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#port 21
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show context
 bgp neighbor 192.168.13.99
 advertisement-interval 100
 peer-group eBGPPeerGrp1
 port 21
 allowas-in 10
 attribute-unchanged as-path
 capability orf prefix-list both
 default-originate
 description neighbor "This neighbor is an external AS neighbor"
 disable-connected-check
 dont-capability-negotiate
 ebgp-multihop 20
 enforce-multihop
 local-as 20 no-prepend
 maximum-prefix 400 50 warning-only
 next-hop-self
 override-capability
 passive
 password neighbor eBGPneighbor@300
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

### Related Commands

```
no (bgp-neighbor-config) on
page 1921
```

Removes the non-standard port configured for this neighbor

### *remote-as (bgp-neighbor-config)*

Configures the ASN for this neighbor BGP device (or devices using this profile). ASN is a set of routers under the same administration that use IGP (Interior Gateway Protocol) and common metrics to define how to route packets within the AS.

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

### Syntax

```
remote-as <1-4294967295>
```

### Parameters

```
remote-as <1-4294967295>
```

```
remote-as <1-4294967295>
```

Specify the remote ASN from 1 - 4294967295.

### Examples

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#remote-as 100
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show context
 bgp neighbor 192.168.13.99
 remote-as 100
 advertisement-interval 100
```

```

peer-group eBGPPeerGrp1
port 21
allowas-in 10
attribute-unchanged as-path
capability orf prefix-list both
default-originate
description neighbor "This neighbor is an external AS neighbor"
disable-connected-check
dont-capability-negotiate
ebgp-multihop 20
enforce-multihop
local-as 20 no-prepend
maximum-prefix 400 50 warning-only
next-hop-self
override-capability
passive
password neighbor eBGPneighbor@300
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#

```

### Related Commands

|                                                    |                                                                              |
|----------------------------------------------------|------------------------------------------------------------------------------|
| <code>no (bgp-neighbor-config)</code> on page 1921 | Removes the ASN for this neighbor BGP device (or devices using this profile) |
|----------------------------------------------------|------------------------------------------------------------------------------|

### *remove-private-as (bgp-neighbor-config)*

Removes the private ASN from outbound updates. By default private ASNs are included in outbound updates.

Private AS numbers are not advertised to the Internet. This option is used with external BGP (eBGP) peers only. The router removes the AS numbers only if the update includes private AS numbers. If the update includes both private and public AS numbers, the system treats it as an error.

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

### Syntax

```
remove-private-as
```

### Parameters

None

### Examples

```

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#remove-private-as
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show context
 bgp neighbor 192.168.13.99
 remote-as 100
 advertisement-interval 100
 peer-group eBGPPeerGrp1
 port 21
 allowas-in 10
 attribute-unchanged as-path
 capability orf prefix-list both
 default-originate

```

```

description neighbor "This neighbor is an external AS neighbor"
disable-connected-check
dont-capability-negotiate
ebgp-multihop 20
enforce-multihop
local-as 20 no-prepend
maximum-prefix 400 50 warning-only
next-hop-self
override-capability
passive
password neighbor eBGPneighbor@300
remove-private-as
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#

```

## Related Commands

---

### *route-server-client (bgp-neighbor-config)*

Enables this BGP neighbor device (or devices using this profile) to act as a route server client. This option is disabled by default.

#### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

#### Syntax

```
route-server-client
```

#### Parameters

None

#### Examples

```

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#route-server-
client
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show context
 bgp neighbor 192.168.13.99
 remote-as 100
 advertisement-interval 100
 peer-group eBGPPeerGrp1
 port 21
 allowas-in 10
 attribute-unchanged as-path
 capability orf prefix-list both
 default-originate
 description neighbor "This neighbor is an external AS neighbor"
 disable-connected-check
 dont-capability-negotiate
 ebgp-multihop 20
 enforce-multihop
 local-as 20 no-prepend
 maximum-prefix 400 50 warning-only
 next-hop-self
 override-capability
 passive
 password neighbor eBGPneighbor@300
 remove-private-as

```

```
route-server-client
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

## Related Commands

|                                                    |                                                                                                    |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------|
| <code>no (bgp-neighbor-config) on page 1921</code> | Disables this BGP neighbor device (or devices using this profile) to act as a route server client. |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------|

### *send-community (bgp-neighbor-config)*

Enables sending of the community attribute to the BGP neighbor. The community attribute groups destinations in a certain community and applies routing decisions based on the community. On receiving community attribute, the BGP router announces it to the neighbor.

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

### Syntax

```
send-community [both|extended|standard]
```

### Parameters

```
send-community [both|extended|standard]
```

|                                                      |                                                                                                                                                                                                                                       |
|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>send-community [both extended standard]</code> | Enables sending of the community attributes to the BGP neighbor                                                                                                                                                                       |
|                                                      | <ul style="list-style-type: none"><li>• both - Sends extended and standard community attributes</li><li>• extended - Sends extended community attributes only</li><li>• standard - Sends standard community attributes only</li></ul> |

### Examples

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#send-community
both
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show context
 bgp neighbor 192.168.13.99
 remote-as 100
 advertisement-interval 100
 peer-group eBGPPeerGrp1
 port 21
 allowas-in 10
 attribute-unchanged as-path
 capability orf prefix-list both
 default-originate
 description neighbor "This neighbor is an external AS neighbor"
 disable-connected-check
 dont-capability-negotiate
 ebgp-multihop 20
 enforce-multihop
 local-as 20 no-prepend
 maximum-prefix 400 50 warning-only
 next-hop-self
 override-capability
 passive
 password neighbor eBGPneighbor@300
 remove-private-as
 route-server-client
```

```
send-community both
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

### Related Commands

|                                                    |                                                                 |
|----------------------------------------------------|-----------------------------------------------------------------|
| <code>no (bgp-neighbor-config)</code> on page 1921 | Disables sending of the community attribute to the BGP neighbor |
|----------------------------------------------------|-----------------------------------------------------------------|

### *shutdown (bgp-neighbor-config)*

Shuts down this BGP neighbor device (or devices using this profile). When configured, this neighbor is administratively shut down. This option is disabled by default.

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

### Syntax

```
shutdown
```

### Parameters

None

### Examples

```
nx9500-6C8809(config-profile testNX500-router-bgp-neighbor-192.168.13.99)#shutdown
nx9500-6C8809(config-profile testNX500-router-bgp-neighbor-192.168.13.99)#show context
 bgp neighbor 192.168.13.99
 remove-private-as
 route-server-client
 shutdown
nx9500-6C8809(config-profile testNX500-router-bgp-neighbor-192.168.13.99)#
```

### Related Commands

|                                                    |                                                       |
|----------------------------------------------------|-------------------------------------------------------|
| <code>no (bgp-neighbor-config)</code> on page 1921 | Removes the administrative shut down of this neighbor |
|----------------------------------------------------|-------------------------------------------------------|

### *soft-reconfiguration (bgp-neighbor-config)*

Enables storing of updates for inbound soft reconfiguration. This option is disabled by default.

Soft-reconfiguration can be used in lieu of BGP route refresh capability. Enabling this option enables local storage of all received routes and their attributes. This requires additional memory on the BGP device.

When a soft reset (inbound) is performed on the neighbor device, the locally stored routes are reprocessed according to the inbound policy. The BGP neighbor connection is not affected.

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

---

## Syntax

```
soft-reconfiguration inbound
```

## Parameters

```
soft-reconfiguration inbound
```

|                              |                                                                      |
|------------------------------|----------------------------------------------------------------------|
| soft-reconfiguration inbound | Performs a soft reconfiguration (inbound) on the BGP neighbor device |
|------------------------------|----------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#soft-reconfiguration inbound
```

## Related Commands

|                                                       |                               |
|-------------------------------------------------------|-------------------------------|
| <a href="#">no (bgp-neighbor-config)</a> on page 1921 | Disables soft reconfiguration |
|-------------------------------------------------------|-------------------------------|

## *strict-capability-match (bgp-neighbor-config)*

Enforces a strict capability match before allowing a TCP connection with this neighbor. In case capabilities do not match, the BGP connection is not established. This option is disabled by default.

## Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

## Syntax

```
strict-capability-match
```

## Parameters

None

## Examples

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#strict-capability-match
```

## Related Commands

|                                                       |                                                                                    |
|-------------------------------------------------------|------------------------------------------------------------------------------------|
| <a href="#">no (bgp-neighbor-config)</a> on page 1921 | Disables a strict capability match before allowing a connection with this neighbor |
|-------------------------------------------------------|------------------------------------------------------------------------------------|

## *timers (bgp-neighbor-config)*

Configures this BGP neighbor's keepalive and holdtime durations



### Note

The keepalive and holdtime settings configured at the neighbor level override those configured on the BGP router.

---



### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

### Syntax

```
timers [<0-65535> <0-65535>|connect <0-65535>]
```

### Parameters

```
timers [<0-65535> <0-65535>|connect <0-65535>]
```

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| timers <0-65535> <0-65535> | Sets the keepalive and holdtime intervals <ul style="list-style-type: none"><li>• &lt;0-65535&gt; - Specifies the keepalive interval from 0 - 65535 seconds. It is the interval, in seconds, between two successive keepalive packets exchanged with this neighbor to keep the TCP connection alive.</li><li>• &lt;0-65535&gt; - Specifies the holdtime interval from 0 - 65535. This is the time this neighbor will wait without receiving a keepalive packet from its neighbor before declaring it dead. If the time since the last keepalive packet received (from its neighbor) exceeds the value set here, the neighbor is declared dead.</li></ul> |
| timers connect <0-65535>   | Sets the BGP connect time. This is the interval, in seconds, after which BGP tries to connect to a dead peer. <ul style="list-style-type: none"><li>• &lt;0-65535&gt; - Specify a value from 1 - 65535 seconds.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                |

### Examples

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#timers 20 40
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#timers connect
20
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show context
 bgp neighbor 192.168.13.99
 remote-as 100
 advertisement-interval 100
 peer-group eBGPPeerGrp1
 port 21
 strict-capability-match
 timers connect 20
 timers 20 40
 allowas-in 10
 attribute-unchanged as-path
 capability orf prefix-list both
 default-originate
 description neighbor "This neighbor is an external AS neighbor"
 disable-connected-check
 dont-capability-negotiate
 ebgp-multihop 20
 enforce-multihop
 local-as 20 no-prepend
 maximum-prefix 400 50 warning-only
 next-hop-self
 override-capability
 passive
 password neighbor eBGPneighbor@300
 remove-private-as
 route-server-client
 send-community both
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

## Related Commands

|                                                    |                                                  |
|----------------------------------------------------|--------------------------------------------------|
| <code>no (bgp-neighbor-config)</code> on page 1921 | Removes the holdtime value set for this neighbor |
|----------------------------------------------------|--------------------------------------------------|

### *unsuppress-map (bgp-neighbor-config)*

Un-suppresses map to selectively advertise routes that have been suppressed using the aggregate-address command. The aggregate-address command creates a route map with a IP/mask address that consolidates subnets under it. This reduces the number of route maps on the BGP device to one consolidated entry. Use unsuppress-map to selectively allow/deny a subnet or a set of subnets from this consolidated entry.

#### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

#### Syntax

```
unsuppress-map <ROUTE-MAP-NAME>
```

#### Parameters

```
unsuppress-map <ROUTE-MAP-NAME>
```

|                                                    |                                                                                                                                                           |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>unsuppress-map &lt;ROUTE-MAP-NAME&gt;</code> | Un-suppresses the specified route map <ul style="list-style-type: none"><li>• <code>&lt;ROUTE-MAP-NAME&gt;</code> – Specify the route map name.</li></ul> |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Examples

```
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp-neighbor-192.168.13.99#
unsuppress-map test
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp-neighbor-192.168.13.99#show
context
 bgp neighbor 192.168.13.99
 remote-as 199
 maximum-prefix 9999 80 restart 50
 unsuppress-map test
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp-neighbor-192.168.13.99#
```

## Related Commands

|                                                    |                                                                   |
|----------------------------------------------------|-------------------------------------------------------------------|
| <code>no (bgp-neighbor-config)</code> on page 1921 | Removes the 'un-suppress' flag applied on the specified route map |
|----------------------------------------------------|-------------------------------------------------------------------|

### *update-source (bgp-neighbor-config)*

Allows BGP sessions to use any operational interface to establish the TCP connection with this neighbor

#### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

#### Syntax

```
update-source <IPv4>
```

## Parameters

update-source <IPv4>

|                      |                                                  |
|----------------------|--------------------------------------------------|
| update-source <IPv4> | Specify the BGP enabled neighbor's IPv4 address. |
|----------------------|--------------------------------------------------|

## Examples

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#update-source
192.168.13.1
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show context
 bgp neighbor 192.168.13.99
 remote-as 100
 advertisement-interval 100
 peer-group eBGPPeerGrp1
 port 21
 strict-capability-match
 timers connect 20
 timers 20 40
 allowas-in 10
 attribute-unchanged as-path
 capability orf prefix-list both
 default-originate
 description neighbor "This neighbor is an external AS neighbor"
 disable-connected-check
 dont-capability-negotiate
 ebgp-multihop 20
 enforce-multihop
 local-as 20 no-prepend
 maximum-prefix 400 50 warning-only
 next-hop-self
 override-capability
 passive
 password neighbor eBGPneighbor@300
 remove-private-as
 route-server-client
 send-community both
 update-source 192.168.13.1
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

## Related Commands

|                                                    |                                       |
|----------------------------------------------------|---------------------------------------|
| <code>no (bgp-neighbor-config)</code> on page 1921 | Removes the source of routing updates |
|----------------------------------------------------|---------------------------------------|

*use (bgp-neighbor-config)*

Configures filters for this neighbor. These filters are BGP IP ACL, IP prefix list, AS path list, and route map. Based on the filters used, updates received from this neighbor are filtered.

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

## Syntax

```
use [distribute-list <BGP-IP-ACL-NAME>|filter-list <AS-PATH-LIST-NAME>|
prefix-list <IP-PREFIX-LIST-NAME>|route-map <BGP-ROUTE-MAP-NAME>]
```

## Parameters

```
use [distribute-list <BGP-IP-ACL-NAME>|filter-list <AS-PATH-LIST-NAME>|
prefix-list <IP-PREFIX-LIST-NAME>|route-map <BGP-ROUTE-MAP-NAME>]
```

|                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>use [distribute-list &lt;BGP-<br/>IP-ACL-NAME&gt; <br/>filter-list &lt;AS-PATH-LIST-<br/>NAME&gt; <br/>prefix-list &lt;IP-PREFIX-LIST-<br/>NAME&gt; <br/>route-map &lt;BGP-ROUTE-MAP-<br/>NAME&gt;]</pre> | <p>Uses predefined and configured filters with this neighbor</p> <ul style="list-style-type: none"><li>• distribute-list &lt;BGP-IP-ACL-NAME&gt; - Uses a BGP IP ACL<ul style="list-style-type: none"><li>• &lt;BGP-IP-ACL-NAME&gt; - Specify the BGP IP ACL name.</li></ul></li><li>• filter-list &lt;AS-PATH-LIST-NAME&gt; - Uses an AS path list<ul style="list-style-type: none"><li>• &lt;AS-PATH-LIST-NAME&gt; - Specify the AS path list name.</li></ul></li><li>• prefix-list &lt;IP-PREFIX-LIST-NAME&gt; - Uses a IP prefix list<ul style="list-style-type: none"><li>• &lt;IP-PREFIX-LIST-NAME&gt; - Specify the IP prefix list name.</li></ul></li><li>• route-map &lt;BGP-ROUTE-MAP-NAME&gt; - Uses a route map<ul style="list-style-type: none"><li>• &lt;BGP-ROUTE-MAP-NAME&gt; - Specify the route map name.</li></ul></li></ul> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp-neighbor-192.168.13.99)#use
filter-list FilterList_01 in
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp-neighbor-192.168.13.99)#use route-
map testBGPRouteMap out
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp-neighbor-192.168.13.99)#show
context
 bgp neighbor 192.168.13.99
 remote-as 199
 use filter-list FilterList_01 in
 maximum-prefix 9999 80 restart 50
 use route-map testBGPRouteMap out
 unsuppress-map test
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp-neighbor-192.168.13.99)#
```

## Related Commands

|                                                    |                                                                        |
|----------------------------------------------------|------------------------------------------------------------------------|
| <code>no (bgp-neighbor-config)</code> on page 1921 | Removes the filters used to filter updates received from this neighbor |
|----------------------------------------------------|------------------------------------------------------------------------|

### *weight (bgp-neighbor-config)*

Configures a weight for all routes learned from this BGP neighbor. Weight is used to decide the preferred route when the same route is learned from multiple neighbors. The highest weight is always chosen.

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

## Syntax

```
weight <0-65535>
```

## Parameters

```
weight <0-65535>
```

|                                   |                                                                                                                                                                                     |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>weight &lt;0-65535&gt;</pre> | <p>Specifies a relative weightage for all routes learned from this neighbor</p> <ul style="list-style-type: none"><li>• &lt;0-65535&gt; - Specify a value from 0 - 65535.</li></ul> |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Examples

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
weight 10
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show context
 bgp neighbor 192.168.13.99
 remote-as 100
 advertisement-interval 100
 peer-group eBGPPeerGrp1
 port 21
 strict-capability-match
 timers connect 20
 timers 20 40
 allowas-in 10
 attribute-unchanged as-path
 capability orf prefix-list both
 default-originate
 description neighbor "This neighbor is an external AS neighbor"
 disable-connected-check
 dont-capability-negotiate
 ebgp-multihop 20
 enforce-multihop
 local-as 20 no-prepend
 maximum-prefix 400 50 warning-only
 next-hop-self
 override-capability
 passive
 password neighbor eBGPneighbor@300
 remove-private-as
 route-server-client
 send-community both
 update-source 192.168.13.1
 weight 10
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

## Related Commands

|                                                    |                          |
|----------------------------------------------------|--------------------------|
| <code>no (bgp-neighbor-config)</code> on page 1921 | Reverts to default value |
|----------------------------------------------------|--------------------------|

### *no (bgp-neighbor-config)*

Removes this BGP neighbor's settings, or reverts them back to default

### Supported in the following platforms:

- Wireless Controllers — RFS 4000
- Service Platforms — NX 95XX, NX 96XX

### Syntax

```
no <PARAMETER>
```

### Parameters

```
no <PARAMETER>
```

|                                   |                                                              |
|-----------------------------------|--------------------------------------------------------------|
| <code>no &lt;PARAMETER&gt;</code> | Specify the parameter details to remove or revert to default |
|-----------------------------------|--------------------------------------------------------------|

## Examples

The following example shows the neighbor 192.168.13.99 settings before the 'no' commands are executed:

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show context
 bgp neighbor 192.168.13.99
 advertisement-interval 100
 allowas-in 10
 attribute-unchanged as-path
 capability orf prefix-list both
 default-originate
 description neighbor "This neighbor is an external AS neighbor"
 disable-connected-check
 dont-capability-negotiate
 ebgp-multihop 20
 enforce-multihop
 local-as 20 no-prepend
 maximum-prefix 400 50 warning-only
 next-hop-self
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#no
advertisement-interval
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#no disable-
connected-check
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#no default-
originate
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#no local-as
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show
context
 bgp neighbor 192.168.13.99
 allowas-in 10
 attribute-unchanged as-path
 capability orf prefix-list both
 description neighbor "This neighbor is an external AS neighbor"
 dont-capability-negotiate
 ebgp-multihop 20
 maximum-prefix 400 50 warning-only
 next-hop-self
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

# CONTROLLER MANAGED WLAN USE CASE

## CREATING A FIRST CONTROLLER MANAGED WLAN

This section describes the process of creating managed WLAN on an RFS 4000 wireless controller, and associating it with the AP 7161 and AP 7602 access points.

Upon completion, you will have created a WLAN on a RFS 4000 model wireless controller using a DHCP server to allocate IP addresses to associated wireless clients.

### Assumptions

Verify the following conditions have been satisfied before attempting the WLAN configuration activities described in this section:

- It is assumed the RFS 4000 wireless controller has the latest firmware version available.
- It is assumed the AP 7161 and AP 7602 access points also have the latest firmware version available.
- It is assumed there are no previous configurations on the wireless controller or access point and default factory configurations are running on the devices.
- It is assumed you have administrative access to the wireless controller and access point CLI.
- It is assumed the individual administrating the network is a professional network installer.

### Designs

This section defines the network design being implemented.



**Figure 1: Network Design**

---

This is a simple deployment scenario, with the Access Points connected directly to the wireless controller. One wireless controller port is connected to an external network.

On the RFS 4000 wireless controller, the GE1 interface is connected to an external network. Interfaces GE3 and GE4 are used by the Access Points.

On the external network, the wireless controller is assigned an IP address of 192.168.10.188. The wireless controller acts as a DHCP server for the wireless clients connecting to it, and assigns IP addresses in the range of 172.16.11.11 to 172.16.11.200. The rest of IPs in the range are reserved for devices requiring static IP addresses.

## Using the Command Line Interface to Configure the WLAN

These instructions are for configuring your first WLAN using the wireless controller CLI.

Use a serial console cable when connecting to the wireless controller for the first time. Set the following configuration when using the serial connection:

- Bits per second: *19200*
- Data Bit: *8*
- Parity: *None*
- Stop Bit: *1*
- Flow Control: *None*

## Logging into the Controller for the First Time

When powering on the wireless controller for the first time, you are prompted to replace the existing administrative password. The credentials for logging into the wireless controller for the first time are:

- User Name: *admin*
- Password: *admin123*

Ensure the new password created is strong enough to provide adequate security for the wireless controller managed network.

After logging in to the controller, follow the steps below to configure a controller-managed WLAN:

- 1 [Create an RF Domain.](#)
- 2 [Create a controller profile, with WLAN, VLAN and GE interface configurations.](#)
- 3 [Create an access point profile.](#)
- 4 [Create a DHCP server policy.](#)
- 5 [Test your WLAN status.](#)

## Creating a RF Domain

A RF Domain is a collection of configurations specific to devices located at the same physical deployment, such as a building or a floor. Create a RF Domain and assign the country code where the devices are deployed. Configuring the country code is mandatory, or else the devices will not function as intended.



The instructions in this section must be performed from the Global Configuration mode of the wireless controller.

- 1 Navigate to the wireless controller's global configuration mode.

```
rfs4000>enable
rfs4000#
rfs4000#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
rfs4000(config)#
```

- 2 Create the RF Domain using the following commands:

```
rfs4000(config)#rf-domain <RF-DOMAIN-NAME>
rfs4000(config)#rf-domain RFDOMAIN_UseCase1
rfs4000(config-rf-domain-RFDOMAIN_UseCase1)#
```

This command creates a profile with the name RFDOMAIN\_UseCase1.

- 3 Set the RF Domain's country code (location of deployment).

```
rfs4000(config-rf-domain-RFDOMAIN_UseCase1)#country-code us
```

This sets the country code for this RF Domain. Save this change and exit the RF Domain configuration context.

```
rfs4000(config-rf-domain-RFDOMAIN_UseCase1)#commit write
rfs4000(config-rf-domain-RFDOMAIN_UseCase1)#exit
rfs4000(config)#
```

- 4 Apply the RF Domain to the wireless controller's self context.

```
rfs4000(config)#self
rfs4000(config-device-03-14-28-57-14-28)#
rfs4000(config-device-03-14-28-57-14-28)#use rf-domain RFDOMAIN_UseCase1
```

- 5 Commit the changes and write to memory. Exit this context.

```
rfs4000(config-device-03-14-28-57-14-28)#commit write memory
rfs4000(config-device-03-14-28-57-14-28)#exit
rfs4000(config)#
```

## Creating a Wireless Controller Profile

The first step in creating a WLAN is to configure a profile defining the parameters applied to a wireless controller.

- 1 **Creating A Profile.** To create a profile:

```
rfs4000(config)#profile rfs4000 RFS4000_UseCase1
rfs4000(config-profile-RFS4000_UseCase1)#
```

This creates a profile with the name *RFS400\_UseCase1* and moves the cursor into its context. Any configuration made under this profile is available when it is applied to a device.

- 2 **Configuring a VLAN on the Profile.** Create the VLAN to use with the WLAN configuration. In this example, we are configuring VLAN 2.

```
rfs4000(config-profile-RFS4000_UseCase1)#interface vlan 2
rfs4000(config-profile-RFS4000_UseCase1-if-vlan2)#ip address 172.16.11.1/24
```

The above command assigns the IP address 172.16.11.1 with the mask of 255.255.255.0 to VLAN2. Exit the VLAN2 context.

```
rfs4000(config-profile-RFS4000_UseCase1-if-vlan2)#exit
rfs4000(config-profile-RFS4000_UseCase1)#
```

- 3 **Mapping the configured VLAN to a physical interface.**

---

The next step is to assign this newly created VLAN to a physical interface. In this case, VLAN 2 is mapped to GE3 and GE4 to support two access points, an AP 7602 and AP 7161. The AP 7602 is connected to the gigabit interface GE3 and the AP 7161 to the GE4 interface.

- a Navigate to the physical interface's configuration context, as shown in the following example:

```
rfs4000(config-profile-RFS4000_UseCase1)#interface ge 3
rfs4000(config-profile-RFS4000_UseCase1-if-ge3)#
```

- b Map VLAN 2 to this interface. This assigns the IP address to the selected physical interface

```
rfs4000(config-profile-RFS4000_UseCase1-if-ge3)#switchport access vlan 2
rfs4000(config-profile-RFS4000_UseCase1-if-ge3)#exit
rfs4000(config-profile-RFS4000_UseCase1)#
```

- c Similarly, map the defined VLAN 2 to the GE4 interface.

```
rfs4000(config-profile-1_UseCase1)#interface ge 4
rfs4000(config-profile-RFS4000_UseCase1-if-ge4)#switchport access vlan 2
rfs4000(config-profile-RFS4000_UseCase1-if-ge4)#exit
rfs4000(config-profile-RFS4000_UseCase1)#
```

- 4 Save changes and Exit the profile configuration context.

```
rfs4000(config-profile-RFS4000_UseCase1)#exit
rfs4000(config)#commit write memory
```

- 5 **Applying the profile to the controller.** Before the wireless controller can be further configured, the profile must be applied to the wireless controller.

```
rfs4000(config)#self
rfs4000(config-device-03-14-28-57-14-28)#
rfs4000(config-device-03-14-28-57-14-28)#use profile RFS4000_UseCase1
rfs4000(config-device-03-14-28-57-14-28)#exit
rfs4000(config)#commit write
```

- 6 **Creating a WLAN.** Use the following commands to create a WLAN and configure it's mandatory parameters:

- a Create a WLAN.

```
rfs4000(config)#wlan 1
rfs4000(config-wlan-1)#
```

- b Configure the WLAN's SSID. This is the value that identifies and helps differentiate this WLAN.

```
rfs4000(config-wlan-1)#ssid WLAN_USECASE_01
```

- c Enable the SSID to be broadcasted so that wireless clients can find it and associate.

```
rfs4000(config-wlan-1)#broadcast-ssid
```



#### Note

The WLAN created for this usecase, is an *open* WLAN, with no authentication mode specified. Once the WLAN is mapped to an AP, clients will not require password for associating with the WLAN through the AP.

---

- d Associate VLAN 2 to the WLAN and exit.

```
rfs4000(config-wlan-1)#vlan 2
rfs4000(config-wlan-1)#exit
```

- 7 Commit the changes. Once these changes have been made, they have to be committed before proceeding.

```
rfs4000(config)#commit write memory
```

## Creating an AP Profile

An AP profile provides a method of applying common settings to Access Points of the same model. The profile significantly reduces the time required to configure Access Points within a large deployment.

For more information, see:

- [Creating an AP 7161 Profile](#) on page 1927
- [Creating a AP 7602Profile](#) on page 1928

### Creating an AP 7161 Profile

Follow the steps below to configure a AP 7161 profile:

- 1 In the wireless controller's global config mode, create a AP 7161 profile.
 

```
rfs4000(config)#profile ap7161 AP7161_UseCase1
rfs4000(config-profile-AP7161_UseCase1)#
```
- 2 Assign the profile to the VLAN defined in [Creating a Wireless Controller Profile](#). In this section, the VLAN was defined as VLAN 2. When applied to the AP 7161 access point, this profile will configure the AP to be a member of VLAN 2.
 

```
rfs4000(config-profile-AP7161_UseCase1)#interface vlan 2
rfs4000(config-profile-AP7161_UseCase1-if-vlan2)#
```
- 3 Configure this VLAN to use DHCP. Enabling DHCP on the VLAN ensures that devices associating using this access point are automatically assigned a unique IP address. Once completed, exit this context.
 

```
rfs4000(config-profile-AP7161_UseCase1-if-vlan2)#ip address dhcp
rfs4000(config-profile-AP7161_UseCase1-if-vlan2)#exit
```
- 4 Map the VLAN to a physical interface on the profile. In this example, VLAN 2 is mapped to the GE1 and GE2 interfaces of the AP profile. When applied to the AP 7161 access point, this profile will map VLAN 2 to the AP's GE1 and GE2 ports.
 

```
rfs4000(config-profile-AP7161_UseCase1)#interface ge 1
rfs4000(config-profile-AP7161_UseCase1-if-ge1)#switchport access vlan 2
rfs4000(config-profile-AP7161_UseCase1-if-ge1)#exit
```
- 5 Similarly configure the GE2 interface.
 

```
rfs4000(config-profile-AP7161_UseCase1)#interface ge 2
rfs4000(config-profile-AP7161_UseCase1-if-ge2)#switchport access vlan 2
rfs4000(config-profile-AP7161_UseCase1-if-ge2)#exit
```
- 6 Map the WLAN to a radio on the access point. An AP 7161 has 3 radios (on certain models), two of which can be configured for WLAN support. In this scenario, two radios 1 and 2 are mapped to [WLAN '1' created earlier](#).
 

```
rfs4000(config-profile-AP7161_UseCase1)#interface radio 1
rfs4000(config-profile-AP7161_UseCase1-if-radio1)#wlan 1
rfs4000(config-profile-AP7161_UseCase1-if-radio1)#exit
rfs4000(config-profile-AP7161_UseCase1)#interface radio 2
rfs4000(config-profile-AP7161_UseCase1-if-radio2)#wlan 1
rfs4000(config-profile-AP7161_UseCase1-if-radio2)#exit
rfs4000(config-profile-AP7161_UseCase1)#
```
- 7 Commit the changes made to the profile and exit this context.
 

```
rfs4000(config-profile-AP7161_UseCase1)#commit write
rfs4000(config-profile-AP7161_UseCase1)#exit
rfs4000(config)#
```
- 8 Apply this profile to the discovered AP 7161.
  - a Use the discovered AP 7161's MAC address to access the AP's configuration context, as shown here.
 

```
rfs4000(config)#ap7161 00-23-68-16-C6-C4
rfs4000(config-device-00-23-68-16-C6-C4)#
```
  - b Assign the profile to the AP 7161access point.
 

```
rfs4000(config-device-00-23-68-16-C6-C4)#use profile AP7161_UseCase1
rfs4000(config-device-00-23-68-16-C6-C4)#commit write
```
  - c Apply the RF Domain to the AP 7161access point.

Apply the [previously created RF Domain](#) to enable a country code to be assigned to the discovered access point. A discovered access point only works properly if its country code is the same as its associated wireless controller.

```
rfs4000(config-device-00-23-68-16-C6-C4)#use rf-domain RFDOMAIN_UseCase1
rfs4000(config-device-00-23-68-16-C6-C4)#commit write
rfs4000(config-device-00-23-68-16-C6-C4)#Exit
rfs4000(config)#
```

### Creating a AP 7602Profile

An AP 7602's firmware is updated directly by its associated wireless controller. The process is automatic, and no intervention is required.

Follow the steps below to configure an AP 7602 profile:

- 1 In the wireless controller's global config mode, create a AP 7602 profile.

```
rfs4000(config)#profile ap7602 AP7602_UseCase1
rfs4000(config-profile-AP7602_UseCase1)#
```
- 2 Assign the profile to the VLAN defined in [Creating a Wireless Controller Profile](#). In this section, the VLAN was defined as VLAN 2. When applied to the AP 7602 access point, this profile will configure the AP to be a member of VLAN 2.

```
rfs4000(config-profile-AP7602_UseCase1)#interface vlan 2
rfs4000(config-profile-AP7602_UseCase1-if-vlan2)#
```
- 3 Configure this VLAN to use DHCP. Enabling DHCP on the VLAN ensures that devices associating using this access point are automatically assigned a unique IP address. Once completed, exit this context.

```
rfs4000(config-profile-AP7602_UseCase1-if-vlan2)#ip address dhcp
rfs4000(config-profile-AP7602_UseCase1-if-vlan2)#exit
```
- 4 Map the VLAN to a physical interface on the profile. In this example, VLAN 2 is mapped the GE1 interface. When applied to the AP 7602 access point, this profile will map VLAN 2 to the AP's GE1 port.

```
rfs4000(config-profile-AP7602_UseCase1)#interface ge 1
rfs4000(config-profile-AP7602_UseCase1-if-ge1)#switchport access vlan 2
rfs4000(config-profile-AP7602_UseCase1-if-ge1)#exit
```
- 5 Map the WLAN to a radio on the access point. An AP 7602 has 2 radios, in this scenario, both radios are mapped to [WLAN '1' created earlier](#).

```
rfs4000(config-profile-AP7602_UseCase1)#interface radio 1
rfs4000(config-profile-AP7602_UseCase1-if-radio1)#wlan 1
rfs4000(config-profile-AP7602_UseCase1-if-radio1)#exit
rfs4000(config-profile-AP7602_UseCase1)#interface radio 2
rfs4000(config-profile-AP7602_UseCase1-if-radio2)#wlan 1
rfs4000(config-profile-AP7602_UseCase1-if-radio2)#exit
rfs4000(config-profile-AP7602_UseCase1)#
```
- 6 Commit the changes and exit.

```
rfs4000(config-profile-AP7602_UseCase1)#commit write memory
rfs4000(config-profile-AP7602_UseCase1)#exit
rfs4000(config)#
```
- 7 Apply this profile to the discovered AP 7602.
  - a Use the discovered AP 7602's MAC address to access the AP's configuration context, as shown here.

```
rfs4000(config)#ap7602 00-A0-F8-00-00-01
rfs4000(config-device-00-A0-F8-00-00-01)#
```
  - b Assign the profile to this AP 7602access point.

```
rfs4000(config-device-00-A0-F8-00-00-01)#use profile AP7602_UseCase1
rfs4000(config-device-00-A0-F8-00-00-01)#commit write
```

- c Apply the RF Domain profile to the AP.

Apply the previously [created RF Domain](#) to enable a country code to be assigned to the discovered access point. A discovered access point only works properly if its country code is the country code of its associated wireless controller.

```
rfs4000(config-device-00-A0-F8-00-00-01)#use rf-domain RFDOMAIN_UseCase1
rfs4000(config-device-00-A0-F8-00-00-01)#commit write
rfs4000(config-device-00-A0-F8-00-00-01)#exit
rfs4000(config)#
```

## Creating a DHCP Server Policy

The DHCP server policy defines the parameters required to run a DHCP server on the wireless controller and assign IP addresses automatically to devices that associate. Configuring DHCP enables the reuse of a limited set of IP addresses.

To create a DHCP server policy, in the wireless controller’s global configuration mode, execute the following command:

```
rfs4000-37FABE(config)#dhcp-server-policy <DHCP-SERVER-POLICY-NAME>
rfs4000(config)#dhcp-server-policy DHCP_POLICY_UseCase1
rfs4000(config-dhcp-policy-DHCP_POLICY_UseCase1)#
```

The following table displays how IP addresses are used.

*Table: IP Address Usage*

| IP Range                         | Usage                                                             |
|----------------------------------|-------------------------------------------------------------------|
| 172.16.11.1 till 172.16.11.10    | Reserved for devices that require a static IP address             |
| 172.16.11.11 till 172.16.11.200  | Range of IP addresses that can be assigned using the DHCP server. |
| 172.16.11.201 till 172.16.11.254 | Reserved for devices that require a static IP address             |

In the table, the IP address range of 172.16.11.11 to 172.16.11.200 is available using the DHCP server. To configure the DHCP server:

```
rfs4000(config-dhcp-policy-DHCP_POLICY_UseCase1)#dhcp-pool DHCP_POOL_USECASE1_01
rfs4000(config-dhcp-policy-DHCP_POLICY_UseCase1-pool-DHCP_POOL_USECASE1_01)#
```

- 1 Configure the address range as follows:

```
rfs4000(config-dhcp-policy-DHCP_POLICY_UseCase1-pool-DHCP_POOL_USECASE1_01)#address
range 172.16.11.11 172.16.11.200
rfs4000(config-dhcp-policy-DHCP_POLICY_UseCase1-pool-DHCP_POOL_USECASE1_01)#
```

- 2 Configure the IP pool used with a network segment. This starts the DHCP server on the specified interface.

```
rfs4000(config-dhcp-policy-DHCP_POLICY_UseCase1-pool-DHCP_POOL_USECASE1_01)#network
172.16.11.0/24
rfs4000(config-dhcp-policy-DHCP_POLICY_UseCase1-pool-DHCP_POOL_USECASE1_01)#exit
rfs4000(config-dhcp-policy-DHCP_POLICY_UseCase1)#exit
rfs4000(config)#commit write
```

- 3 Configure the RFS 4000 to use the DHCP Policy. For the DHCP to work, apply the policy to the wireless controller, as shown in the following example:

```
rfs4000-37FABE(config)#self
rfs4000-37FABE(config-device-03-14-28-57-14-28)#use dhcp-server-policy
DHCP_POLICY_UseCase1
rfs4000-37FABE(config-device-03-14-28-57-14-28)#commit write
```

---

```
rfs4000-37FABE(config-device-03-14-28-57-14-28)#exit
rfs4000-37FABE(config)#
```

## Completing and Testing the Configuration

Once your WLAN is up, test it using any mobile unit (example, mobile phone or laptop).

- Ensure that your mobile unit is Wi-Fi enabled.
- Search for the WLAN\_USECASE\_01 ssid. This is the SSID of the controller-managed WLAN created and mapped to the access points.
- Click **Connect**. You should get internet access.